

**CAN AMERICANS TRUST THE PRIVACY
AND SECURITY OF THEIR
INFORMATION ON HEALTHCARE.GOV?**

JOINT HEARING
BEFORE THE
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
&
SUBCOMMITTEE ON OVERSIGHT
COMMITTEE ON SCIENCE, SPACE, AND
TECHNOLOGY
HOUSE OF REPRESENTATIVES
ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

FEBRUARY 12, 2015

Serial No. 114-6

Printed for the use of the Committee on Science, Space, and Technology



Available via the World Wide Web: <http://science.house.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

93-884PDF

WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HON. LAMAR S. SMITH, Texas, *Chair*

FRANK D. LUCAS, Oklahoma	EDDIE BERNICE JOHNSON, Texas
F. JAMES SENSENBRENNER, JR.	ZOE LOFGREN, California
DANA ROHRABACHER, California	DANIEL LIPINSKI, Illinois
RANDY NEUGEBAUER, Texas	DONNA F. EDWARDS, Maryland
MICHAEL T. MCCAUL	FREDERICA S. WILSON, Florida
STEVEN M. PALAZZO, Mississippi	SUZANNE BONAMICI, Oregon
MO BROOKS, Alabama	ERIC SWALWELL, California
RANDY HULTGREN, Illinois	ALAN GRAYSON, Florida
BILL POSEY, Florida	AMI BERA, California
THOMAS MASSIE, Kentucky	ELIZABETH H. ESTY, Connecticut
JIM BRIDENSTINE, Oklahoma	MARC A. VEASEY, TEXAS
RANDY K. WEBER, Texas	KATHERINE M. CLARK, Massachusetts
BILL JOHNSON, Ohio	DON S. BEYER, JR., Virginia
JOHN R. MOOLENAAR, Michigan	ED PERLMUTTER, Colorado
STEVE KNIGHT, California	PAUL TONKO, New York
BRIAN BABIN, Texas	MARK TAKANO, California
BRUCE WESTERMAN, Arkansas	BILL FOSTER, Illinois
BARBARA COMSTOCK, Virginia	
DAN NEWHOUSE, Washington	
GARY PALMER, Alabama	
BARRY LOUDERMILK, Georgia	

SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY

HON. BARBARA COMSTOCK, Virginia, *Chair*

FRANK D. LUCAS, Oklahoma	DANIEL LIPINSKI, Illinois
MICHAEL T. MCCAUL, Texas	ZOE LOFGREN, California
STEVEN M. PALAZZO, Mississippi	SUZANNE BONAMICI, Oregon
RANDY HULTGREN, Illinois	KATHERINE M. CLARK, Massachusetts
JOHN R. MOOLENAAR, Michigan	SUZANNE BONAMICI, Oregon
STEVE KNIGHT, California	DON S. BEYER, JR., Virginia
BRUCE WESTERMAN, Arkansas	EDDIE BERNICE JOHNSON, Texas
GARY PALMER, Alabama	
LAMAR S. SMITH, Texas	

SUBCOMMITTEE ON OVERSIGHT

HON. BARRY LOUDERMILK, Georgia, *Chair*

F. JAMES SENSENBRENNER, JR.,	DON BEYER, Virginia
Wisconsin	ALAN GRAYSON, Florida
BILL POSEY, Florida	ZOE LOFGREN, California
THOMAS MASSIE, Kentucky	EDDIE BERNICE JOHNSON, Texas
JIM BRIDENSTINE, Oklahoma	
BILL JOHNSON, Ohio	
LAMAR S. SMITH, Texas	

CONTENTS

February 12, 2015

Witness List	Page 2
Hearing Charter	3

Opening Statements

Statement by Representative Barbara Comstock, Chairwoman, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	8
Written Statement	9
Statement by Representative Daniel Lipinski, Ranking Minority Member, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	10
Written Statement	11
Statement by Representative Barry Loudermilk, Chairman, Subcommittee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives	12
Written Statement	14
Statement by Representative Don S. Beyer, Ranking Minority Member, Sub- committee on Oversight, Committee on Science, Space, and Technology, U.S. House of Representatives	15
Written Statement	16

Witnesses:

Ms. Michelle De Mooy, Deputy Director, Consumer Privacy, Center for De- mocracy and Technology	
Oral Statement	18
Written Statement	21
Mr. Morgan Wright, Principal, Morgan Wright, LLC	
Oral Statement	32
Written Statement	34
Discussion	46

Appendix I: Answers to Post-Hearing Questions

Ms. Michelle De Mooy, Deputy Director, Consumer Privacy, Center for De- mocracy and Technology	62
Mr. Morgan Wright, Principal, Morgan Wright, LLC	65

Appendix II: Additional Material for the Record

Prepared statement by Representative Elizabeth Esty, Committee on Science, Space, and Technology, U.S. House of Representatives	68
Letters submitted by Representative Barbara Comstock, Chairwoman, Sub- committee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	69
Documents submitted by Representative Barbara Comstock, Chairwoman, Subcommittee on Research and Technology, Committee on Science, Space, and Technology, U.S. House of Representatives	83

**CAN AMERICANS TRUST THE PRIVACY
AND SECURITY OF THEIR
INFORMATION ON HEALTHCARE.GOV?**

THURSDAY, FEBRUARY 12, 2015

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY &
SUBCOMMITTEE ON OVERSIGHT
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
Washington, D.C.

The Subcommittees met, pursuant to call, at 2:49 p.m., in Room 2318 of the Rayburn House Office Building, Hon. Barbara Comstock [Chairwoman of the Subcommittee on Research and Technology] presiding.

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371

www.science.house.gov

Subcommittee on Research and Technology
Subcommittee on Oversight

***Can Americans Trust the Privacy and Security of their
Information on HealthCare.gov?***

Thursday, February 12, 2015

2:00 p.m. to 4:00 p.m.

2318 Rayburn House Office Building

Witnesses

***Ms. Michelle De Mooy, Deputy Director, Consumer Privacy, Center for
Democracy and Technology***

Mr. Morgan Wright, Principal, Morgan Wright, LLC

U.S. HOUSE OF REPRESENTATIVES
 COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
 SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
 SUBCOMMITTEE ON OVERSIGHT

Can Americans Trust the Privacy and Security of their Information on HealthCare.gov?

Thursday, February 12, 2015
 2:00 p.m. – 4:00 p.m.
 2318 Rayburn House Office Building

Purpose

On Thursday, February 12, 2015, the Research and Technology Subcommittee and the Oversight Subcommittee will hold a joint hearing titled *Can Americans Trust the Privacy and Security of their Information on HealthCare.gov?* The hearing stems from recent news reports¹ that dozens of data firms have embedded connections on HealthCare.gov, and that through these connections, the companies could potentially collect and sell personal health, financial, and other information from citizens through the HealthCare.gov website. The hearing will examine both the privacy implications to consumers' personal information from the presence of the companies connected to HealthCare.gov, and whether these third party connections add vulnerabilities to the website's security.

A broader question related to the hearing is why the U.S. government would allow data-mining companies such open access to such personal data flowing through HealthCare.gov or any government website. Given the President's Executive Order on Open Data issued in May 2013 calling for departments and agencies of the federal government to be "more accessible to the public and to entrepreneurs,"² was it also properly communicated that the government should also take steps "appropriately safeguarding sensitive information and rigorously protecting privacy"?³

Witnesses

- **Ms. Michelle De Mooy**, Deputy Director, Consumer Privacy, Center for Democracy and Technology
- **Mr. Morgan Wright**, Principal, Morgan Wright, LLC

Overview

On January 20, 2015, the *Associated Press* reported that when consumers "apply for coverage on HealthCare.gov, dozens of data companies may be able to tell that you are on the site. Some can even glean details such as your age, income, ZIP code, whether you smoke or if you are pregnant."⁴ The news report identifies "50 third-party connections embedded on HealthCare.gov,"⁵ and quotes a staff

¹ Ricardo Alonzo-Zaldivar and Jake Gillum, "New Privacy Concerns Over Government's Health Care Website," *Associated Press*, January 20, 2015, available at: http://apnews.myway.com/article/20150120/us--health_overhaul-privacy-8b7c5d925b.html; hereinafter AP News Report.

² OSTP Initiatives, available at: <http://www.whitehouse.gov/administration/eop/ostp/initiatives#Openness>; hereinafter OSTP Initiatives.

³ Ibid.

⁴ AP News Report, *supra*, note 1.

⁵ Ibid.

technologist from the Electronic Frontier Foundation, a civil liberties group, as saying, “Third-party embedded websites are troubling because they can be used to track you and track your reading when you’re browsing the Web.”⁶

In addition to these privacy concerns, the presence of the high number of embedded connections on HealthCare.gov also raises security concerns, because, as one cybersecurity expert explained, “As I look at vendors on a website...they could be another potential point of failure.”⁷ Ms. Cheri McGuire, vice-president of cybersecurity policy for Symantec Corporation, echoed similar concerns during a hearing last month before the Subcommittee on Research and Technology when she noted, in response to a question, that opening up HealthCare.gov to so many embedded third parties created additional vulnerabilities.⁸

While a CMS spokesman defended the practice by claiming that “outside vendors ‘are prohibited from using information from these tools on HealthCare.gov for their companies’ purposes,”⁹ the Administration “did not explain how it ensures that privacy and security policies are being followed.”¹⁰

Since the AP’s report last month, private cybersecurity experts, online privacy advocates, and the House Energy & Commerce Committee¹¹ have also confirmed that HealthCare.gov has facilitated embedded connections for data companies that enable them to receive the website users’ personal and health care information automatically.

Background

FISMA

The data on HealthCare.gov is one of the largest collections of personal information ever assembled, linking information from seven different federal agencies along with state agencies and government contractors. Federal agencies have a duty to ensure that these private records have sufficient protection from misuse and security breaches under the Federal Information Security Management Act of 2002 (FISMA), which requires all federal agencies to develop and implement programs that secure their information and information systems.

The National Institute of Standards and Technology (NIST), “develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and in managing cost-effective programs to protect their information and information systems.”¹² Each agency’s information control system must be reviewed, certified and accredited under NIST publication SP 800-37, “Guide for the Security Certification and Accreditation of Federal Information Systems.”¹³ Security

⁶ Ibid.

⁷ Ibid.

⁸ House Science, Space, and Technology Subcommittee on Research and Technology hearing, “The Expanding Cyber Threat,” January 27, 2015, available at: <http://science.house.gov/hearing/subcommittee-research-and-technology-hearing-expanding-cyber-threat>; hereinafter Research and Technology Subcommittee Hearing.

⁹ AP News Report, *supra*, note 1.

¹⁰ Ibid.

¹¹ House Energy and Commerce Committee, “House and Senate Committee Leaders Press Administration on HealthCare.gov Security,” January 30, 2015, available at: <http://energycommerce.house.gov/press-release/house-and-senate-committee-leaders-press-administration-healthcaregov-security>.

¹² NIST, Information Technology Laboratory, Computer Security Division, Computer Security Resource Center, FISMA Compliance, available at: <http://csrc.nist.gov/groups/SMA/fisma/compliance.html>.

¹³ NIST Special Publication 800-37, “Guide for the Security Certification and Accreditation of Federal Information Systems,” May 2004, available at: <https://www.fismacenter.com/SP800-37-final.pdf>.

accreditation is required under OMB Circular A-130, Appendix III. Accredited systems must be monitored continuously, including ongoing assessment of security controls. By accrediting an agency's information system, the responsible agency official "accepts responsibility for the security of the system and is fully *accountable* for any adverse impacts to the agency if a breach of security occurs."¹⁴

Under FISMA, the Director of the Office of Management and Budget (OMB) is required to oversee the information security policies and practices of federal agencies, which include "assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems."¹⁵

NIST Cybersecurity Framework

In February 2013, President Obama issued Executive Order 13636 on cybersecurity for critical infrastructure, which states that it is "the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."¹⁶

The Executive Order describes critical infrastructure as, "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."¹⁷ The Executive Order also directed NIST to "lead the development of a framework to reduce cyber risks to critical infrastructure,"¹⁸ and in February 2014, NIST released the *Framework for Improving Critical Infrastructure Cybersecurity*¹⁹ (Framework).

NIST worked in collaboration with industry stakeholders to establish this three-pronged document that includes a Core, Profile and Implementation Tiers. "The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure."²⁰ The Framework also assists "organizations in incorporating privacy and civil liberties as part of a comprehensive cybersecurity program."²¹ During the Research and Technology Subcommittee hearing previously referenced, another witness, Dr. Charles Romine from NIST, noted in response to a question that the Framework "does have a pretty strong statement to say about privacy, and NIST has embarked on a privacy engineering research activity partly as a result of what we learned from the framework process, that there needs to be more guidance and more tools available for people to promote privacy considerations."²²

¹⁴ Ibid; (Emphasis in original).

¹⁵ Public Law 107-347, available at: <http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>

¹⁶ Executive Order – Improving Critical Infrastructure Cybersecurity, February 12, 2013, available at: <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

¹⁷ Ibid.

¹⁸ Ibid.

¹⁹ National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0, February 12, 2014, available at: <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.

²⁰ Ibid.

²¹ Ibid.

²² Research and Technology Subcommittee Hearing, *supra*, note 8.

Government Reports

Various reports issued in the past few months by federal watchdog agencies have identified privacy and security concerns about HealthCare.gov. For example, a GAO report from last fall identified weaknesses “in the processes used for managing information security and privacy as well as the technical implementation of IT security controls.”²³ More recently, a report²⁴ from the U.S. Department of Health and Human Services’ Office of Inspector General revealed contract planning and procurement failures, which also raises questions about the ability of HealthCare.gov to protect consumers’ private and sensitive information.

Health Care Breaches

Last September, news organizations reported that a “hacker broke into part of the HealthCare.gov insurance enrollment website in July and uploaded malicious software.”²⁵ And as recently as last week, consumers learned about what is being described as perhaps the largest data breach against a health care company when Anthem Inc., the country’s second-biggest health insurer, was attacked. Anthem disclosed that “names, birth dates, Social Security numbers, medical IDs, street and e-mail addresses and employee information including income levels were stolen”²⁶ for 80 million Anthem members. This has prompted the suggestion that consumers should closely monitor their medical statements because medical or “health-insurance information can sell for 10 times what a credit card number fetches on the black market, making it a lucrative area for cybercriminals.”²⁷

Open Data Policy

The broader question is why the Administration decided to share such private consumer data from American citizens who were required to register for HealthCare.gov. On May 9, 2013, the Administration issued a memorandum on open data policy noting that, “Information is a valuable national resource and a strategic asset to the Federal Government, its partners, and the public. In order to ensure that the Federal Government is taking full advantage of its information resources, executive departments and agencies... must manage information as an asset throughout its life cycle to promote openness and interoperability, and properly safeguard systems and information.”²⁸

The President also issued an Executive Order the same day to establish an Open Data Policy to make “open and machine-readable data the new default for government information, taking historic steps

²³ U.S. Government Accountability Office, “HealthCare.gov: Actions Needed to Address Weaknesses in Information Security and Privacy Controls, Report GAO-14-730, September 2014, available at: <http://www.gao.gov/assets/670/665840.pdf>.

²⁴ U.S. Department of Health and Human Services, Office of Inspector General, “Federal Marketplace: Inadequacies in Contract Planning and Procurement,” Report OEI-03-14-00230, January 2015, available at: <https://oig.hhs.gov/oei/reports/oei-03-14-00230.pdf>.

²⁵ Danny Yadron, “Hacker Breached HealthCare.gov Insurance Site,” *The Wall Street Journal*, September 4, 2014, available at: <http://online.wsj.com/articles/hacker-breached-healthcare-gov-insurance-site-1409861043>.

²⁶ Shannon Pettypiece, “What to do Right Now If You’re One of the 80 Million Anthem Members Who Got Hacked,” *Bloomberg*, February 5, 2015, available at: http://finance.yahoo.com/news/now-youre-one-80-million-214043538.html?_ylt=A0LEVv1K4tZU124ALt0nnlIQ.

²⁷ Ibid.

²⁸ Office of Management and Budget Memorandum (M-13-13), From Sylvia Burwell, OMB Director, Steven VanRoekel, Federal Chief Information Officer, Todd Park, U.S. Chief Technology Officer and Dominic J. Mancini, Acting Administrator, Office of Information and Regulatory Affairs, May 9, 2013, available at: <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf>.

to make government-held data more accessible to the public and to entrepreneurs while appropriately safeguarding sensitive information and rigorously protecting privacy.”²⁹ This situation with HealthCare.gov seems to indicate that the Administration was more interested in providing government-held data to entrepreneurs for the purposes of data-mining than in protecting privacy.

However, an interim progress report released last week, spearheaded by John Podesta, counselor to the President, raises serious privacy concerns related to big data technologies. In response to a request from President Obama for a “wide-ranging review of big data and privacy,”³⁰ the report notes:

“While there are promising technological means to better protect privacy in a big data world, the report’s authors concluded these methods are far from perfect, and technology alone cannot protect privacy absent strong social norms and a responsive policy and legal framework. Finally, the report raised issues around other values potentially implicated by big data technology—particularly with regard to the potential for big data technologies to lead, purposely or inadvertently, to discriminatory outcomes on the basis of race, gender, socioeconomic status, or other categories.”³¹

In a parallel effort, the Podesta report was supported by the President’s Council of Advisors on Science and Technology (PCAST) “to investigate the scientific and technological dimensions of big data and privacy.”³² In a report issued last year, the Council notes:

“The challenges to privacy arise because technologies collect so much data (e.g., from sensors in everything from phones to parking lots) and analyze them so efficiently (e.g., through data mining and other kinds of analytics) that it is possible to learn far more than most people had anticipated or can anticipate given continuing progress. These challenges are compounded by limitations on traditional technologies used to protect privacy (such as de-identification). PCAST concludes that technology alone cannot protect privacy, and policy intended to protect privacy needs to reflect what is (and is not) technologically feasible.”³³

Against this backdrop, the hearing will examine the privacy and cybersecurity questions raised by the embedded connections of dozens of third party data firms on HealthCare.gov.

²⁹ OSTP Initiatives, *supra*, note 2.

³⁰ John Podesta, Counselor to the President, Penny Pritzker, Dept. of Commerce Secretary, Ernest Moniz, Dept. of Energy Secretary, John Holdren, OSTP Director, Jeff Zients, Economic Advisor to the President, Interim Progress Report, “Big Data: Seizing Opportunities, Preserving Values,” February 2015, available at: http://www.whitehouse.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf.

³¹ *Ibid.*

³² *Ibid.*

³³ PCAST Report to the President, “Big Data and Privacy: A Technological Perspective,” May 2014, available at: http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

Chairwoman COMSTOCK. The Subcommittee on Research and Technology and Subcommittee on Oversight will come to order.

Without objection, the Chair is authorized to declare recesses of the Subcommittee at any time.

Good afternoon. Welcome to today's hearing entitled "Can Americans Trust the Privacy and Security of Their Information on Healthcare.gov?"

In front of you are packets containing the written testimony, biographies, and truth-in-testimony disclosures for today's witnesses.

I recognize myself for five minutes for an opening statement.

Now, the reason we are having the hearing today is just over three weeks ago on January 20, the Associated Press reported that as many as 50 data mining companies had access to consumers' personal and health information on HealthCare.gov. Companies such as Google, Twitter, Facebook, Yahoo, and Advertising.com apparently were provided access by CMS, the Centers for Medicare and Medicaid Services.

Upon learning of this development, Chairman Smith sent several letters to department heads questioning the practice and trying to get more information about what actually had happened, but no one has replied with additional information at this point.

As reported by AP, "When you apply for coverage on HealthCare.gov, dozens of data companies may be able to tell that you are on the site." While the information shared with these third party companies does not include, apparently, the healthcare consumer's Social Security number, it appears that a number of data companies may have had access to consumers' age, income, ZIP code, smoking practices, pregnancy status, and even computer IP address.

While some may characterize this as a harmless collection of data, it can actually be more revealing. A recent MIT study of credit card data revealed that only four pieces of outside information about a user, including one's social media activity, were sufficient to identify a person in the database of a million people.

The concerns with HealthCare.gov's practice of sharing data are twofold. There are privacy implications of feeding consumers' personal data—unbeknownst to them—to third party vendors, and there are security concerns, because additional connections to the website can lead to additional vulnerabilities.

During my first hearing that we had here on the Subcommittee I shared that I experienced a credit card breach because someone had ordered \$7,000 of products and wrongfully charged them to my credit card right before Christmas. Fortunately, that situation resolved fairly quickly and I wasn't liable for those charges, but what if the information stolen had been about healthcare? How would that impact somebody?

You know, you can get a new credit card but when that is taken or hacked, like whatever happened in that case, but once personal health information is compromised, personal family information, other things like that, you don't know where that may go and it could be out there forever. That is why health and health insurance information apparently is reportedly worth up to 10 times as much as credit card information on the black market.

The risks posed by HealthCare.gov data-sharing are underscored by the fact that a hacker accessed the website last July to upload malicious software. Government investigators found no evidence that consumers' personal data were taken, but HHS said the attack appears to have been the first successful intrusion into the website. Many security experts have warned of vulnerability to hacking since HealthCare.gov went live more than a year ago.

And just last week, we learned about what might be the largest data breach against the country's second biggest health insurer, Anthem. In this case, stolen information for 80 million Anthem members included names, birth dates, Social Security numbers and medical IDs. That impacted my constituents so I, and I know other colleagues of mine in Virginia, posted information about the Anthem situation at my official website to inform our constituents, but obviously they had very strong concerns when healthcare information may be at risk.

Today's hearing is a precursor to one at which we will invite witnesses from the federal government to answer specific questions about the HealthCare.gov contracts with the third party companies. I look forward to the insights of both our witnesses today as the Committee continues its due diligence over this issue.

And I do want to emphasize that obviously we do want to hear from the folks at CMS and the Chairman had reached out to them, but we wanted to proceed and hear from other experts such as are here today.

[The prepared statement of Mrs. Comstock follows:]

PREPARED STATEMENT OF SUBCOMMITTEE
CHAIRWOMAN BARBARA COMSTOCK

Three weeks ago, on January 20, the Associated Press reported that as many as 50 data mining companies had access to consumers' personal and health information on HealthCare.gov. Companies such as Google, Twitter, Facebook, Yahoo, and Advertising.com apparently were provided access by CMS (the Centers for Medicare and Medicaid Services).

As reported by AP, "When you apply for coverage on HealthCare.gov, dozens of data companies may be able to tell that you are on the site." While the information shared with these third party companies does not include the health care consumer's Social Security number, it appears that a number of data companies may have had access to consumers' age, income, ZIP code, smoking practices, pregnancy status, and even computer IP address.

While some may characterize this as a harmless collection of data, it can actually be much more revealing. A recent MIT study of credit card data revealed that only four pieces of outside information about a user, including one's social media activity, were sufficient to identify a person in the database of a million people.

The concerns with HealthCare.gov's practice of sharing data with companies like Google, Twitter and Facebook are two-fold. There are privacy implications of feeding consumers' personal data—unknownst to them—to third party vendors, and there are security concerns, because additional connections to the website can lead to additional vulnerabilities.

We also should consider this news in the context of President Obama's announcement that he would bring forward a new online privacy and cybersecurity proposal later this month. This proposal was described as building on steps previously taken to "protect American companies, consumers, and infrastructure from cyber threats, while safeguarding privacy and civil liberties." It seems to me that what the AP has reported about Americans' data on HealthCare.gov and what the President expects of Americans may be in conflict or certainly raise legitimate concerns.

Privacy protections at federal government websites should be the gold standard, setting the bar for others to follow. Privacy protections at federal websites should at least follow the guidance provided through the Federal Information Security

Management Act and last year's publication of the Cybersecurity Framework by the National Institute of Standards and Technology. I am interested in hearing from our expert witnesses about privacy protections for users of HealthCare.gov.

During my first hearing as Chairwoman of this Subcommittee, I shared that I experienced a credit card breach because someone had ordered \$7,000 in wrongful charges on my card right before Christmas.

Fortunately, the situation was resolved and I wasn't liable for those charges. But what if information stolen like this had been related to health?

You can get a new credit card when your old one is hacked. But once personal health information is compromised, it could be out there forever. That is why health and health insurance information is reportedly worth up to ten times as much as credit card information on the black market.

The risks posed by HealthCare.gov data sharing are underscored by the fact that a hacker accessed the website last July to upload malicious software. Government investigators found no evidence that consumers' personal data were taken, but HHS said the attack appears to have been the first successful intrusion into the website. Many security experts have warned of vulnerability to hacking since HealthCare.gov went live more than a year ago.

And just last week, we learned about what might be the largest data breach against the country's second biggest health insurer, Anthem. In this case, stolen information for 80 million Anthem members included names, birth dates, Social Security numbers and medical IDs.

I posted information about the Anthem situation at my official website to inform my constituents.

Today's hearing is a precursor to one at which we will invite witnesses from the federal government to answer specific questions about the HealthCare.gov contracts with third party companies. I look forward to the insights of both our witnesses today as the Committee continues its due diligence over this issue.

Chairwoman COMSTOCK. Now, before I yield to the Ranking Member, I ask unanimous consent that the following documents be placed in the record, which include the letters from Chairman Smith I referenced earlier.

Without objection, there we go.

[The information appears in Appendix II]

Chairwoman COMSTOCK. Now, I recognize the Ranking Member of the Research and Technology Subcommittee, the gentleman from Illinois, Mr. Lipinski, for his opening statement.

Mr. LIPINSKI. Thank you, Madam Chairwoman.

I want to welcome the witnesses to this afternoon's hearing.

I am troubled by some of the things we know and some of the things we don't know about privacy and security on HealthCare.gov. We have a couple of very good witnesses today who I look forward to hearing from. Unfortunately, neither of these experts had any role in developing HealthCare.gov or decisions regarding privacy and security, but I do hope that the testimony will help shape some of the questions we should be asking those who did have a role in those decisions.

Given the problematic rollout of HealthCare.gov and problems with some state exchange websites such as those with the D.C. marketplace, it is clear that the implementation of the technical side of the Affordable Care Act merits Congressional review and oversight. While HealthCare.gov functionality has improved since last year and CMS has been responsive to reports of potential security or privacy weaknesses as they have been identified, we should continue to conduct oversight because the type of personal data that is inputted into the site raises the potential for serious problems.

Yet we must also make sure that we are clear on the context. We are here today because of recent news reports about the use of

third-party analytics tools on HealthCare.gov, as the Chairwoman mentioned. Data analytics tools can be valuable for tracking how websites are being used and optimizing the website for the consumer. While I am on the record about my reservations about the Affordable Care Act, I also understand the motivation of increasing traffic to the HealthCare.gov website in an effort to get more people signed up for health insurance.

However, we must hold the government to the highest standards for privacy and security. This is especially true for a website like HealthCare.gov in which people enter highly private and sensitive information. I have concerns based on the initial news reports that the high standards may not have been applied to privacy on HealthCare.gov. However, the news reports, like today's testimony, have provided more questions than answers. We must also be careful to distinguish between privacy and security and where the true vulnerabilities may be for each. In short, we have a responsibility to gather all the facts before coming to any conclusions but we need to get those facts.

I understand, Madam Chairwoman, that you are trying to schedule a second hearing with Administration officials who have direct knowledge of the issues before us today. I think such a hearing, in addition to more staff homework, will be necessary before we can draw any clear conclusions or proposals for moving forward.

In addition, I would note that privacy is a big issue across the internet. Data analytics tools can help improve customer experience but their ubiquity and integration into the working of so many websites means that Americans concerned about their privacy may have little real choice when it comes to how they can manage the release of their information. Ms. De Mooy addresses some of that in her testimony and I look forward to the discussion on the broader issues. While we may hold the government to higher standards, it is incumbent upon us to declare the steps we can take to ensure that Americans are able to safeguard their personal data across the online environment as a whole.

Finally, while this hearing will focus on online data privacy, it is critical to recognize that using the internet is far from the only way for Americans' private information to be lost. In his testimony, Mr. Wright addresses the difficulty of anonymizing data and the ease with which individuals can be identified from just a few pieces of information about their day-to-day activities such as purchases charged through a credit card. Given this testimony, this Committee may want to be careful about efforts to publicly disclose study data related to the health impacts of the air pollutants used in the EPA regulation. It is an issue that we debated in the last Congress and I think this is something that we need to consider, the problems with anonymizing data, as we move forward.

I look forward to hearing from the witnesses today, and with that, I yield back.

[The prepared statement of Mr. Lipinski follows:]

PREPARED STATEMENT OF SUBCOMMITTEE
MINORITY RANKING MEMBER DANIEL LIPINSKI

Thank you Madam Chairwoman. I want to welcome the witnesses to this morning's hearing on privacy and security on the healthcare.gov website.

I am troubled by some of the things we know and some of the things we don't know about privacy and security on healthcare.gov. We have some very good witnesses today who I look forward to hearing from. Unfortunately none of these experts had any role in developing healthcare.gov or in the decisions regarding privacy and security. I do hope the testimony will help shape some of the questions we should be asking those who did have a role in those decisions.

Given the problematic rollout of healthcare.gov and problems with some state exchange websites such as those with the DC marketplace, it's clear that the implementation of the technical side of the Affordable Care Act merits Congressional review and oversight. While healthcare.gov functionality has improved since last year and CMS has been responsive to reports of potential security or privacy weaknesses as they have been identified, we should continue to conduct oversight because the type of personal data that is input into the site raises the potential for serious problems.

Yet we must also make sure that we are clear on the context. We are here today because of recent news reports about the use of third-party analytics tools on healthcare.gov. Data analytics tools can be valuable for tracking how websites are being used and optimizing the website for the consumer. While I am on the record about my own reservations about the Affordable Care Act, I also understand the motivation of increasing traffic to the healthcare.gov website in an effort to get more people signed up for health insurance.

However, we must hold the government to the highest standards for privacy and security. This is especially true for a website like healthcare.gov in which people enter highly private and sensitive information. I have concerns, based on the initial news reports, that the highest standards may not have been applied to privacy on healthcare.gov. However, the news reports, like today's testimony, provide more questions than answers. We must also be careful to distinguish between privacy and security, and where the true vulnerabilities may be for each. In short, we have a responsibility to gather all of the facts before coming to any conclusions. But we need those facts.

I understand, Madam Chairwoman, that you are trying to schedule a second hearing with Administration officials who have direct knowledge of the issues before us today. I think such a hearing, in addition to more staff homework, will be necessary before we can draw any clear conclusions or proposals for moving forward.

In addition, I would note that privacy is a big issue across the internet. Data analytics tools can help improve customer experience. But their ubiquity and integration into the workings of so many websites means that Americans concerned about their privacy may have little real choice when it comes to how they can manage the release of their information. Ms. De Mooy addresses some of that in her testimony and I look forward to a discussion on the broader issues. While we may hold the government to a higher standard, it is incumbent upon us to consider steps we can take to ensure that Americans are able to safeguard their personal data across the online environment as a whole.

Finally, while this hearing will focus on online data privacy, I think it is critical to recognize that using the internet is far from the only way for Americans' private information to be lost. In his testimony, Mr. Wright addresses the difficulty of anonymizing data and the ease with which individuals can be identified through just a few pieces of information about their day-to-day activities, such as purchases charged to a credit card. Given this testimony, this Committee may want to be careful about efforts to publicly disclose study data related to the health impacts of air pollutants used in EPA regulations.

I look forward to hearing from the experts before us today and with that I yield back.

Chairwoman COMSTOCK. I now recognize the Chair of the Oversight Subcommittee, the gentleman from Georgia, Mr. Loudermilk, for an opening statement.

Mr. LOUDERMILK. Thank you, Chairwoman Comstock. I appreciate the opportunity to be here, and welcome to all of our witnesses here today. And I am looking forward to hearing from each of you as we gather information on this very important issue.

Just last week, I joined many of my Republican colleagues to vote for a full repeal of ObamaCare. This sweeping healthcare law has punished countless Americans by doubling some health insur-

ance costs for the same or less coverage in many cases by no longer being able to use the plans they were promised to keep.

That same healthcare law created HealthCare.gov, a federally operated health insurance exchange website to assist Americans in signing up for healthcare coverage. As reported by the Associated Press on January 20, 2015, dozens of companies, including Google, Facebook, and Twitter, had embedded connections to HealthCare.gov. Essentially, when a consumer was applying for coverage on the website, it is possible that some or all of those data companies were able to tell, at the very least, when a person was on the site, their age, their income, their ZIP code, and whether they smoked or even if they were pregnant.

The Centers for Medicare and Medicaid Services claim that this kind of data mining is necessary for data analytics in order to improve user experience. If that is the case, however, I wonder why the number of embedded connections to the website has significantly dropped since the first news story on the matter. Did the Administration actually know and approve all the companies that were connected to HealthCare.gov?

One of our witnesses here today comes from the Center for Democracy and Technology, which compiles similar analytics in-house instead of through a slew of different companies. This technique decreases privacy and security vulnerabilities by giving website access to a minimum number of individuals who are able to improve user experience without compromising user information.

Having multiple outside connections to HealthCare.gov means more vendors have access to the website, which only means one thing: increased vulnerabilities. About one year ago, hackers were able to use just one vendor, an HVAC company based in Pennsylvania, to obtain credit and debit card information of millions of Target customers nationwide.

Cybercriminals appear to be increasingly interested in the personal information collected by U.S. insurers, so much so that a recent Reuters article warned that 2015 could be “the Year of the Healthcare Hack.” So far, it looks as though they are right. Just last week, it was disclosed that a database containing personal information for about 80 million customers of health insurer Anthem, Incorporated, was hacked. It is feared that this breach exposed names, birthdays, addresses, and Social Security numbers—all information that HealthCare.gov website requests of its customers.

As someone with a background in the IT sector, I find what appears to be extensive tracking of Americans’ personal information extremely disconcerting and unnecessary. Americans were first misled when their President told them “if you like your healthcare insurance plan, you can keep it,” and now it seems like they are being misled into thinking that their personal information on HealthCare.gov is as secure as it can be.

Considering that HealthCare.gov is one of the largest collections of personal information ever assembled, it is extremely important that the Administration implements best practices to protect Americans’ privacy. This Administration ultimately has a responsibility to ensure that personal data collected is secure, and Congressional oversight will continue until the Administration has proved that it is doing all it can to protect the American people.

I look forward to today's hearing where I hope to gain some insight from our expert witnesses on the possible reasoning for why scores of data mining companies would be embedded on HealthCare.gov, as well as the potential consequences of them having access to the website. The American people deserve to know the truth and are owed some level of transparency from this Administration as to how their information on HealthCare.gov is being collected, used, and secured.

Madam Chair, I yield back my time.

[The prepared statement of Mr. Loudermilk follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON OVERSIGHT
CHAIRMAN BARRY LOUDERMILK

Thank you, Chairwoman Comstock, and welcome to all of our witnesses here today. I am looking forward to hearing from each of you as we gather information on this very important issue.

Just last week, I joined many of my Republican colleagues to vote for a full repeal of Obamacare. This sweeping health care law has punished countless Americans by doubling some health insurance costs for the same or less coverage, or, in many cases, by no longer being able to use the plans they were promised to keep.

That same health care law created HealthCare.gov, a federally-operated health insurance exchange website to assist Americans in signing up for healthcare coverage. As reported by the Associated Press on January 20th, 2015, dozens of companies, including Google, Facebook, and Twitter had embedded connections to HealthCare.gov. Essentially, when a consumer was applying for coverage on the website, it is possible that some or all of those data companies were able to tell, at the very least, when the person was on the site, their age, their income, their ZIP code, and whether they smoked or even if they were pregnant.

The Centers for Medicare and Medicaid Services claims that this kind of data mining is necessary for data analytics in order to improve user experience. If that is the case, however, I wonder why their number of embedded connections to the website has significantly dropped since the first news story on this matter. Did the Administration actually know and approve all of the companies that were connected to HealthCare.gov?

One of our witnesses here today comes from the Center for Democracy and Technology, which compiles similar analytics in-house instead of through a slew of different companies. This technique decreases privacy and security vulnerabilities by giving website access to a minimum number of individuals who are able to improve user experience without compromising user information.

Having multiple outside connections to HealthCare.gov means more vendors have access to the website, which only means one thing: increased vulnerabilities. About one year ago, hackers were able to use just one vendor, an HVAC Company based in Pennsylvania, to obtain the credit and debit card information of millions of Target customers nation-wide.

Cybercriminals appear to be increasingly interested in the personal information collected by U.S. insurers, so much so that a recent Reuters article warned that 2015 could be "the Year of the Healthcare Hack." So far, it looks as though they are right. Just last week, it was disclosed that a database containing personal information for about 80 million customers of health insurer Anthem, Inc. was hacked. It is feared that this breach exposed names, birthdays, addresses, and Social Security numbers—all information that the HealthCare.gov website requests of its customers.

As someone with a background in the IT sector, I find what appears to be extensive tracking of Americans' personal information extremely disconcerting and unnecessary. Americans were first misled when their President told them that, "if you like your health insurance plan, you can keep it," and now it seems like they are being misled into thinking that their personal information on HealthCare.gov is as secure as it can be.

Considering that HealthCare.gov is one of the largest collections of personal information ever assembled, it is extremely important that the Administration implements best practices to protect Americans' privacy. This Administration ultimately has a responsibility to ensure that personal data collected is secure, and Congress-

sional oversight will continue until the Administration has proved that it is doing all it can to protect the American people.

I look forward to today's hearing where I hope to gain some insight from our expert witnesses on the possible reasoning for why scores of data mining companies would be embedded on HealthCare.gov as well as the potential consequences of them having access to the website. The American people deserve to know the truth and are owed some level of transparency from this Administration as to how their information on HealthCare.gov is being collected, used, and secured.

Chairwoman COMSTOCK. Thank you.

I now recognize the Ranking Member of the Subcommittee on Oversight, the gentleman from Virginia and my neighbor, Mr. Beyer, for an opening statement.

Mr. BEYER. Thank you, Madam Chair Comstock, and Chairman Loudermilk for holding this hearing today.

Recent news stories on the sharing of the HealthCare.gov visitor data with third parties really does raise very legitimate privacy concerns. According to these news reports, which we have heard, various personal data was being provided at multiple third-party websites and application tools embedded in the website. No personally identifiable information was provided to third parties but news reports also suggest that the information was being provided to third parties without the clear consent or any knowing consent of the visitors to the site.

I think there are many questions that the Members on both sides of the aisle have about HealthCare.gov implementing the use of third-party tools. What restrictions were placed on the use of this data by third parties? Was there even a need for third-party tools on the website? How do these tools improve the function of the website, users' experience? Could some of this work have been done in-house?

Unfortunately, we are not going to be able to get definitive answer to those questions today. I understand the majority invited government witnesses but they deferred citing too short notice to prepare their testimony. My understanding is they will be coming again later with the proper set of government witnesses to address these issues. In a perfect world, we would have had that first but right now I guess we have to deal with a lot of speculation and discover the government facts later.

The use of third-party website tools on HealthCare.gov has drawn an awful lot of public attention but I hope our witnesses, particularly Ms. De Mooy, can help us explore the larger privacy issues involved.

The use of third-party websites is worrisome but it is certainly not unusual in the digital online environment. One recent study found that the top 100 most popular websites were being monitored by more than 1,300 firms deploying these third-party tools. And while I believe we should definitely explore the privacy implications of using the third-party websites, this too is only a small part of the privacy pie.

From the moment we enter the digital domain, whether it is turning on our cell phone, logging onto the internet, opening up a tablet or other digital device, our data is collected, collated, and analyzed by corporations, organizations, government agencies, and particularly online advertising companies. In the physical world, our identities are often measured by details on our driver's li-

censes, birthday, height, gender, weight, but in the digital world, the metrics used to measure who we are seem to be based on observing the web pages we visit, the purchases we make, the people we personally socialize, the news items we read, and the movies we watch. And I am concerned about the use of these new metrics that constantly track and measure our personal lives online.

On the security side, we should also realize that any IT infrastructure is constantly evolving and improving. It is unclear if the use of third-party tools have any direct impact yet at least on the security of HealthCare.gov but also need this—this needs to be put in perspective. Chairman Loudermilk mentioned Anthem’s recent breach exposing the accounts of 80 million customers. That is eight times the number of people who have signed up through—for the Affordable Care Act through HealthCare.gov.

Since the launch of HealthCare.gov, an additional 10 million Americans have healthcare coverage, and I believe that extending these healthcare market opportunities to 10 million Americans is a tremendously positive event for millions of families across the country. So we have very dark conjectures around the security of the website which we must address, but we also can’t—must keep all of this in perspective about the millions of families who have been helped.

I hope this hearing helps us explore these broad privacy issues and I look forward to hearing from our witnesses. I yield back, Mr. Chair—Madam Chair.

[The prepared statement of Mr. Beyer follows:]

PREPARED STATEMENT OF SUBCOMMITTEE ON OVERSIGHT
RANKING MINORITY MEMBER DON S. BEYER

Thank you Madam Chair Comstock and Chairman Loudermilk for holding this hearing today.

Recent news stories on the sharing of Healthcare.gov visitor data with third parties raise legitimate privacy concerns. According to these news reports data including an individual’s income, zip code and pregnancy status were being provided to multiple Third-Party Websites and Applications (TPWAs) tools embedded on the website. According to these stories, no personally identifiable information, known as PII, was provided to third parties. However, news reports also suggest that the information was being provided to third parties without the clear consent of visitors to the site.

There are many questions I think Members on both sides of the aisle have about how Healthcare.gov implemented the use of third party tools on the website. What restrictions were placed on the use of this data by third parties? Why was there a need for multiple third party tools on the website? How did these tools help improve the function of the website and the user’s experience? Could some of this work have been done in-house?

Unfortunately we will not be able to get definitive answers on any of these questions today. Today’s hearing will be largely speculative in nature since we don’t have any government witnesses to explain these issues. I understand the Majority originally invited government witnesses, but provided them with short notice to prepare their testimony. My understanding is we may have a follow-up hearing with the proper set of witnesses to address these issues

later this month. In a perfect world, we would have had that hearing first. Instead, I fear we will start with lots of speculation and will then try to uncover the facts at a later date.

The use of third party website tools on Healthcare.gov has drawn the public's attention to this issue, but I hope our witnesses, particularly Ms. De Mooy, can help us explore the larger privacy issues regarding the use of these and other tools to monitor online activities and their impact on our individual privacy. The use of third party websites is worrisome, but not unusual in the digital online environment. One recent study, for instance, found that the top 100 most popular websites were being monitored by more than 1,300 firms deploying these third party tools. And while I believe we should explore the privacy implications of using third party websites this is simply a small slice of the privacy pie. From the moment we enter the digital domain, whether it is turning on our cell phone, logging onto the Internet or opening up a tablet or other digital device our data is collected, collated and analyzed by corporations, organizations, government agencies and online advertising companies.

In the physical world our identities are often measured by the details on our driver's licenses: our birth date, our height, our weight and gender. But in the digital world the metrics used to measure who we are seem to be based on observing the web pages we visit, the purchases we make, the people we "virtually" socialize with, the news items we read and the movies we watch. I am concerned about the use of these new metrics that constantly track and measure our personal lives online.

On the security side, we must realize that any IT infrastructure is constantly evolving and improving. It is unclear if the use of third party tools had any direct impact on the security of Healthcare.gov, but I also believe this issue needs to be put in perspective. Just last week, reports surfaced that Anthem, Inc., one of the country's largest health care providers, announced that they had a data breach exposing the accounts of 80 million customers. That breach compromised PII that included customer social security numbers and e-mail addresses. The size of that breach is eight times the total number of people who have signed up for the Affordable Care Act through Healthcare.gov.

Since the launch of Healthcare.gov an additional 10 million Americans now have healthcare coverage. I believe that extending market opportunities to 10 million Americans to get health insurance represents a tremendously positive event for millions of families across this country. Despite the dark conjectures about security of the website, they have not suffered any significant loss of personally identifiable information or major security breach to date.

Privacy protections must be addressed and improved throughout the internet, and that includes on Healthcare.gov. I hope this hearing helps us explore these broad privacy issues and I look forward to hearing from our witnesses.

With that I yield.

Chairwoman COMSTOCK. Thank you.

And if there are Members who wish to submit additional opening statements, your statements will be added to the record at this point.

Chairwoman COMSTOCK. Okay. At this time I would like to introduce our witnesses. Our first witness is Ms. Michelle De Mooy, Deputy Director of the Consumer Privacy Projects at the Center for Democracy and Technology, or CDT. Prior to CDT, Ms. De Mooy was Senior Associate for National Priorities at Consumer Action, a national nonprofit focused on empowering underserved and disadvantaged consumers. Ms. De Mooy earned her bachelor of arts degree in government from Lehigh University.

Our second witness today is Mr. Morgan Wright, Principal from Morgan Wright, LLC, where he provides advisory and consulting services in cybersecurity and identity theft. Mr. Wright has provided in-service training to the FBI Computer Analysis Response Team, served as Global Industry Solutions Manager for Public Safety and Homeland Security at Cisco, and as Vice President of Global Public Safety at Alcatel-Lucent. Mr. Wright received his bachelor of science from Fort Hays State University and an Executive Certificate in Leadership and Management from the University of Notre Dame. Perhaps most important of all, Mr. Wright is a resident of the 10th District of Virginia, but I didn't know you were coming today until they reached out. But I am pleased to welcome you today to the hearing.

So pursuant to Committee's rules, all witnesses must be sworn in before they testify so I guess we all stand up. And please rise and raise your right hand.

Do you solemnly swear or affirm that the testimony that you are about to give will be the truth, the whole truth, and nothing but the truth so help you God?

Let the record reflect that the witnesses answered in the affirmative.

Thank you. You can be seated.

Okay. And now we will have our five-minute statements from the witnesses. And your entire statement, if it is longer, will be entered into the record also.

I now recognize Ms. De Mooy for five minutes to present her testimony.

**TESTIMONY OF MS. MICHELLE DE MOOY,
DEPUTY DIRECTOR, CONSUMER PRIVACY,
CENTER FOR DEMOCRACY AND TECHNOLOGY**

Ms. DE MOOY. Chairwoman Comstock, Chairman Loudermilk, Ranking Member Lipinski, Ranking Member Beyer, and Members of the Committee, thank you for the opportunity to come here today and testify on behalf of the Center for Democracy and Technology.

CDT is a nonpartisan, nonprofit technology policy advocacy organization dedicated to protecting civil liberties and human rights on the internet, including privacy, free expression, and access to information. I currently serve as the Deputy Director of CDT's Consumer Privacy Project.

We welcome the attention the Committee has given to be pressing issues of consumer data privacy and security through the lens of data sharing on HealthCare.gov. I will review first the data-sharing practices on HealthCare.gov, discuss the privacy and security concerns that these bring up, and make five concrete recommendations for the government to address these concerns.

Several weeks ago, the security firm Catchpoint Systems found that user information was being shared with over 50 entities on HealthCare.gov without user knowledge or permission. When citizens visit HealthCare.gov to learn more about the programs offered to them under the Affordable Care Act, they are asked to give certain pieces of personal information order to show which health insurance plans they qualify for. After submitting this information, HealthCare.gov then surprisingly sent a referral URL to an array of third parties that included some of this information that the consumers had submitted to the site, including parental status, ZIP code, and annual income. This information is used both by websites themselves and third parties for website analytics, as well as for advertising and marketing purposes, also known as retargeting.

For HealthCare.gov administration officials have said that the refer URL was directed to third parties in order to give consumers a simpler, more streamlined, and intuitive experience, and this is doubtless true. However, the government's decision to work with outside vendors allowed private companies to access user information without their knowledge or consent. It is not clear if HealthCare.gov used tracking technologies for retargeting purposes but it appears likely to have played a role.

The use of retargeting in order to increase awareness of and enrollment in available health insurance plans would have been an understandable goal for the government. It is not, however, a free pass for the government to share user information and characteristics with an array of third-party commercial entities, without permission.

Sharing of personal information with third parties is a privacy concern for several reasons. People who visit government websites often do not have a choice. They must visit a designated online place in order to access specific government products and services. Personal data is valuable. When personal information is collected and shared, it is often combined with other data to build individual profiles. This profile is used to target products and services to you and is increasingly also used to create consumer scores that function similarly to credit scores. Health information in particular is sold for a high premium on underground markets, some experts estimate up to \$40 to \$50 a record, because it is fairly easy to monetize for criminals seeking to bill expensive medical items to Medicaid, for example, or to commit medical identity theft. The theft or use of health information is much harder to recognize and stop than the theft of financial data and more difficult for victims to seek redress.

The number of third-party content providers loading code into the browsers of visitors on HealthCare.gov poses serious security issues. Researchers have pointed to third-party content as one of the primary ways for websites to be infected with malware. Hackers wishing to compromise the integrity of third-party content providers can accomplish a wide range of attacks from simply changing the content of the page to capturing user information and credentials like passwords.

There is no evidence that personal information from HealthCare.gov has been misused but the number of outside par-

ties that can load content and that can see personal information about users is troubling.

Overall, the privacy and security missteps taken by HealthCare.gov were avoidable. We recommend that the government immediately take the following steps: 1) follow sensible guidance available to them and to Office of Management and Budget documents on third-party sharing; 2) implement the six recommendations to protect user privacy and security on HealthCare.gov made in a 2014 report by the Government Accountability Office; 3) strengthen HealthCare.gov's privacy policy limiting third-party sharing only to which it needs to function; 4) implement in-house analytic software that does not report user data back to the software maker; 5) honor the wishes of consumers that express a preference in their browsers not to be tracked.

Ultimately, Congress can best protect consumer information by strengthening legal incentives for companies to better safeguard data and by enacting comprehensive data privacy legislation to give users more control over how their information is collected and used.

Thank you.

[The prepared statement of Ms. De Mooy follows:]



1634 Eye Street, NW
Suite 1100
Washington, DC 20006

Statement of **Michelle Kathleen De Mooy**
Deputy Director, Consumer Privacy Project
Center for Democracy & Technology

Before the United States House of Representatives Committee on Science,
Space, and Technology, Subcommittee on Research and Technology,
Subcommittee on Oversight

**Can Americans Trust the Privacy and Security of Their Information on
HealthCare.gov?**

February 12, 2015

Chairman Smith, Ranking Member Johnson, Chairwoman Comstock, Chairman
Loudermilk and members of the Committee:

Thank you for the opportunity to testify today on behalf of the Center for
Democracy & Technology. CDT is a nonpartisan, non-profit technology policy
advocacy organization dedicated to protecting civil liberties and human rights on
the Internet, including privacy, free speech, and access to information. I currently
serve as the Deputy Director of CDT's Consumer Privacy Project, which focuses
on developing privacy safeguards for consumers through a combination of legal,
technical, and self-regulatory measures. Ensuring that services are designed in
ways that preserve privacy, establishing protections that apply across the life
cycle of consumers' data, and giving consumers control over how their data is
used are key elements of protecting privacy in the digital age.

We welcome the attention the Committee has given to the pressing issues of
consumer data privacy and security through the lens of data sharing on
HealthCare.gov. CDT's testimony today will briefly describe current data
collection and information sharing practices, how HealthCare.gov employs
collection and sharing, and describe the associated privacy and security
concerns. I will finish with policy and technical recommendations.

I. Data collection and sharing online

There are several layers of communication taking place each time an individual
accesses a website. Some of these layers happen behind the scenes, without a
user's express engagement, and some are more direct. Direct website interaction
includes filling out a forms or signing into accounts. These interactions typically
give consumers a fairly commonsense notice of the information they are sharing.
Not all direct interactions are quite this clear. For example, a consumer may not
know that user names or email logins may be used to link consumers visits
across different websites.

A less obvious, but similarly straightforward, communication occurs when individuals choose to visit a website. The action of clicking on a link or typing in an address triggers a message from your browser to the intended website's server. This action essentially announces your arrival, while sharing basic information like your IP address—just like your phone number is your address on the telephone network, your IP address is your address on the Internet—in order to correctly load the site on your browser. Information exchanged during this process serves a utilitarian purpose—for example, the server needs to know which language you speak and what kind of graphics your computer will allow you to see in order to load the site correctly. Often, the basic information exchanged in this process is used to recognize you and customize your experience in subsequent visits. Information about users is often sent via a referer header, which acts as a kind of sign that people unknowingly carry around online as they surf. This sign lists the last websites that the person has visited and is used both by websites themselves and third parties, such as advertising companies. The information that is exchanged is called the referring URL and it sometimes includes browsing and search information that has directly been encoded into the web link.

On a level less visible to consumers, websites use tracking technology to get a more detailed look at them. To do this, they employ different methods to record a user's behavior as he or she navigates that particular site and even on other websites. Generally speaking, technologies on a website that record behavior and track users across visits (and across different websites) are what we mean when we refer to tracking technology.

There are many types of tracking technologies, each with slightly different properties¹ but all serving the same general purpose of identifying an individual website visitor across time – an important distinction is made between first party tracking, or the capture of information by the website itself, while third party tracking is when other entities, typically unknown to the consumer, are contracted by the website to do analytics or other purposes. The most well known example of a tracking technology is a cookie, or a small file containing identifying information, that is stored on a computer at the request of a website's server – depending on your browser settings, you may be asked for permission for the server to do this but you may not, and it's fair to say that many times users are unaware it is occurring. Cookies are often used to improve the online experience by reducing loading speed and storing preferences like login information or remembering abandoned shopping carts. And when cookies from the same company appear on multiple websites—such as when an analytics company or

¹ For general descriptions of tracking software, see "*Know your Elements*," a website by Ghostery. <http://www.knowyourelements.com/>. Visited on Feb 10, 2015. Some pieces of tracking software are more easily blocked by users, such as those with the ability to clear cookies from a browser. This has prompted an arms race of sorts with increasingly sophisticated tracking tools, such as super cookies, being downloaded by unsuspecting users.

ad network services several distinct sites—that company can correlate your activity across multiple different web contexts in ways that consumers might find unwanted or surprising. The information conveyed by browsing habits is used to develop a marketing profile of an individual: this might include the types of websites and pages a consumer visits, as well as any web searches such as those for information on particular diseases or pharmaceuticals. This information can then be combined with offline data such as address, income, marital status, and prescription drug history to form a dossier. In this way, information about health-related information can be collected and interpreted solely in the context of a person's website browsing and searching habits.

It's important to note that the presence of tracking software may be justified, depending on the circumstances—many websites collect this type of information in order to observe the profile of visitors to their own site, something referred to as web analytics. CDT doesn't use cookies or third parties to perform analytics, but we do look at the log files generated by our servers to get a sense of what content people are interested in and where our visitors come from. Many other commercial and non-commercial sites feel comfortable using third party analytics providers; this results in sharing information about site visitors with companies with which the user has no awareness or relationship.

Whether the site itself or a service provider collects the data, performing web analytics are a key part of the online ecosystem. They allow websites to be responsive to their users interests and intentions in using their website – for example, HealthCare.gov may use web analytics to determine if visitors want to learn information eligibility right away and be directed instead to information about plan rates. The goal of digital analytics is to optimize the site so visitors will want so that they will stay on their site longer, viewing more advertising or buying more products in the case of e-commerce sites, or making it easier for people to enroll in an insurance plan in the case of HealthCare.gov.

Retargeting, also known as remarketing, is a cookie-based advertising technology that allows entities to promote their content they had previously engaged with on other sites around the web. For example, if you looked at a certain pair of shoes on Zappos.com, you might later see a remarketing ad for those same shoes on a different site. To serve these ads, a cookie is placed on a website visitor's computer when they visit a certain site. When these users browse online, this cookie allows that site, and any ad networks with which they do business, to serve them ads based on what they previously did on the original site. The cookie also allows website operators and their advertising partners to know specific details about the visitor such as what products they may have looked at and what they may have placed into a shopping cart. The idea behind retargeting is engaging users in a website by using advertisements that remind them of the products and services they were interested in and converting them into buyers.

II. What happened on HealthCare.gov?

Several weeks ago, the security firm Catchpoint Systems found that user health information was being shared with 50 or more third party entities on HealthCare.gov, without user knowledge or permission. The ensuing media firestorm attracted the attention of privacy and security advocates alike, as well as lawmakers from both sides of the aisle.

When citizens visit HealthCare.gov to learn more about the programs offered to them under the Affordable Care Act, they are asked to give certain pieces of personal information in order to shown which health insurance plans they qualify for in their state. Surprisingly, HealthCare.gov then sent a referer URL to an array of third parties that included, unbeknownst to users, includes some of the information submitted to the site such as parental status, zip code, state and annual income.

Administration officials have said that the referer URL was directed to third parties in order to give consumers a "simpler, more streamlined and intuitive experience" and this is doubtless true. It appears that the designers of HealthCare.gov contracted with third parties primarily with the intention to gain insight into the way the site was being accessed and used. Officials have also said these technologies were used "to get visibility into when consumers are having difficulty, or understand when website traffic is building during busy periods."²

It is true that the technology used on the site can help achieve these internal goals; however, contracting with third parties requires a two-way exchange of information. The government's decision to work with outside vendors allowed private companies to access user health information without knowledge or consent, and without the readily available and easy ability to avoid this exchange. Ad tracking technologies can be used to help advertisers, such as insurance brokers or other health or medical companies, tailor targeted ads solely to people who have visited government healthcare sites and add them to profiles indicating their interest in health insurance or in specific health and medical services. This type of tracking is not just happening on HealthCare.gov – Ghostery recently found many third parties receiving user information on 16 state insurance exchange sites, including personal health information.

The use of re-targeting to increase awareness of and enrollment in available health insurance plans would have been an understandable goal for the government in this case – and it appears likely to have played a role³; however, an understandable goal is not a free pass for the government to share user

² Center for Medicaid and Medicare Services, Press Release, *Protecting Consumer Privacy on HealthCare.gov*, January 24, 2015, <http://www.cms.gov/Newsroom/MediaReleaseDatabase/Press-releases/2015-Press-releases-items/2015-01-24.html>

³ Kaye, Kate, *HealthCare.gov and State Sites Still Crawling with Ad Trackers*, AdAge, February 5, 2015, <http://adage.com/article/privacy-and-regulation/healthcare-gov-state-sites-crawling-ad-trackers/296982/>

information and characteristics with an array of third-party commercial entities without permission from users themselves.

III. Privacy concerns

Sharing of personal information with third parties is a privacy concern for several reasons. People who visit government websites often do not have a choice. They must visit a designated online place in order to access specific government products and services, such as those on HealthCare.gov. For this reason, the government should have been extremely cautious in its approach to third party sharing. Without an easy to implement option to opt-out, users were effectively coerced into agreeing to share personal health information, a clear violation of their expectations. At a minimum they should be given a timely and meaningful understanding of how their data is being collected and used by the website and by any third parties, and they should be given a choice about whether or not this is acceptable, with alternative access to comparable information and services if they choose to opt out.

Because there is a universe of companies that hold volumes of data about individuals, the addition of health information such as pregnancy status rounds out a data profile that can be used for profit. Health information is sold for a high premium on underground markets – some experts estimate as much as \$40-\$50 a record⁴ – because it is fairly easy to monetize for criminals seeking to bill expensive medical items to Medicaid for example or to commit medical identity theft. Unlike financial details about a person, which can be reissued when compromised, health information is more valuable because it changes less often and is not as easy to reissue. Health information is not monitored routinely in the same way that banks monitor financial activity and thus it is harder to recognize theft and harder for consumers to seek redress. Individuals can get a new credit card but it is not as easy to change or obtain a new medical profile.

Some though not all citizens that lack health insurance are from disadvantaged communities, and thus the calculus for deciding on the use of third parties should be weighed towards privacy and away from sharing. Consumers in disadvantaged communities face more potential for harm such as being profiled in data banks as “Rural and Barely Making It,” “Ethnic Second-City Strugglers,” and “Retiring on Empty: Singles.”⁵, categories which a recent Senate Commerce

⁴ Hu, Elise. *Anthem Hacks Renews Calls for Laws to Better Prevent Breaches*. National Public Radio, February 5, 2015.
<http://www.npr.org/blogs/alltechconsidered/2015/02/05/384099135/anthem-hack-renews-calls-for-laws-to-better-prevent-breaches>

⁵ Senate Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations Majority Staff. *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes*, December 18, 2013. Page ii.
http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577

Committee report found. These characterizations may then prompt advertising of the type of subprime mortgage loans and other predatory lending that perpetuates the cycle of poverty.

The online environment is rife with this kind of data collection and sharing and while some companies behave responsibly with user data, many do not. As a steward for consumer protection, we believe the government's online activities should be held to a very high standard. The government should be constrained about the sharing of personal data, should be highly transparent, and should consider doing analytics or retargeting of any kind in-house in order to minimize privacy and security risks.

IV. Security concerns

The number of third-party content providers loading code into the browser of visitors to HealthCare.gov poses serious security issues. Researchers have pointed to third-party content as one of the primary ways for websites to be infected with malware.⁶ Compromising the integrity of third party content providers can accomplish a wide range of attacks, from simply changing the content of the page to capturing user information and credentials like passwords.⁷ There is no evidence that personal information from HealthCare.gov has been misused, but the number of outside parties that can load content (essentially code executed in the browser) and that can see personal health information about users is troubling. Vendors without a direct relationship (and accountability) to the user are often the weakest link in the privacy and security chain.

Malicious code was uploaded to the website in July of 2014⁸, meaning that the web portal was successfully hacked, though authorities maintain that no personal information was stolen at that time. In September of 2014, a Government Accountability Office (GAO) report warned that "increased and unnecessary risks remain of unauthorized access, disclosure or modification of the information collected and maintained by HealthCare.gov." As of February 2015, the GAO's six specific recommendations to improve HealthCare.gov privacy and security appear to not have been fully implemented.

⁶ Provos, Niels, McNamee, Dean, Mavrommatis, Panayiotis, Wang, Ke and Modadugu, Nagendra. *The Ghost In The Browser Analysis of Web-based Malware*. April 2007. https://www.usenix.org/legacy/events/hotbots07/tech/full_papers/provos/provos.pdf

⁷ Grossman, Jeremiah. *Third-Party Web Security FAQ*, July 1, 2010. <http://jeremiahgrossman.blogspot.com/2010/07/third-party-web-widget-security-faq.html>.

⁸ Yadron, Danny. *Hacker Breached HealthCare.gov Insurance Site*. Wall Street Journal, September 4, 2015. <http://www.wsj.com/articles/hacker-breached-healthcare-gov-insurance-site-1409861043>

From the perspective of US Government federal information privacy guidance, there are very few standards or other sources of guidance from agencies like the National Institute of Standards and Technology (NIST) that could be useful for entities like CMS when setting up a complicated information service like healthcare.gov. The most relevant material to privacy guidance is Appendix J of NIST Special Publication 800-53,⁹ a catalog of privacy controls that can be employed beyond security measures to ensure privacy violations are minimized. However, a list of controls without any guidance or framework as how to apply them is limited in value and application. Comprised of a menu of privacy-enhancing tools that federal agency privacy technical folks should consider using in their systems, organizations, and deployments, they are useful but without a framework for practical implementation. There is an ongoing and important NIST effort to create standards for privacy engineering¹⁰ – which would provide the guidance necessary around the controls in Appendix J of SP 800-53 – around a risk assessment framework. While this is a very important effort, it is not yet operational such that federal government designers and engineers could use it while designing and deploying information systems.

V. HealthCare.gov's privacy policy

We believe that HealthCare.gov should have been designed to strictly limit third party data sharing. The practice of sharing with various third parties was, in this case, exacerbated by poor disclosures in the HealthCare.gov privacy policy. HealthCare.gov's privacy policy is quite broad and overly vague, allowing for essentially unlimited user data to be shared with third parties.

Importantly, personally identifiable information (PII) is not defined in the policy. Although the National Institute of Standards and Technology (NIST) has identified data points that should be considered PII, there is no requirement that government agencies or companies adopt NIST's definition. This creates a loophole that, without guidance from HealthCare.gov's privacy policy on what constitutes PII, may allow for some personal information to fall outside the site's policy protections. As the FTC has described, individuals possess an interest in potentially identifiable information beyond "PII,"¹¹ but the Healthcare.gov privacy

⁹ See Appendix J (starting at p. 437) of NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," available at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.

¹⁰ *Privacy Engineering at NIST* homepage. Accessed February 9, 2015. http://csrc.nist.gov/projects/privacy_engineering/index.html

¹¹ Federal Trade Commission, Staff Report. *Self-Regulatory Principles for Online Behavioral Advertising*, February 2009. <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>

policy does not describe or acknowledge the possibility that personal information may be collected without their knowledge through cookies and web logs.

The site policy states that it “uses a variety of technologies and social media services to communicate and interact with citizens” but it is unclear from this policy how extensive these communications are and what citizen information is collected and by whom. The privacy policy should at the least note what information, if any, is typically collected on citizens through third party interactions and how this information is used, stored and shared by HealthCare.gov. Furthermore, the description of use of cookies is, at best, confusing, by conflating first and third-party cookies. HealthCare.gov notes it does not collect personal information through cookies, but it is unclear whether third parties do have access to a HealthCare.gov users’ personal information through cookies. Further, the policy does not place limits on how long collected data may be retained. The policy states that it will keep data “as long as needed to support the mission of the website”. This essentially allows for limitless retention of citizens’ data, which increases the data sets’ vulnerability to hacks.

HealthCare.gov’s privacy policy states “CMS conducts and publishes a Privacy Impact Assessment (PIA) for each use of a third-party website and application (TPWA) as they may have a different functionality or practice. TPWA PIAs are posted for public view on the HHS website at <http://www.hhs.gov/pia>.”

Presumably, any entity that participates in data flows should be subject to a PIA when installed and when changed materially in function, especially if the parties will be involved in directly handling sensitive health information, as was the case here. Therefore, PIAs for all 50 entities found to be sharing information should have been available on HealthCare.gov’s privacy policy; if these PIAs were conducted, they are not readily discoverable on HHS’s PIA website.

The privacy policy also claims that a user should “...review the third-party privacy policies before using the sites and ensure that you understand how your information may be used,” a direction that is both unrealistic and overly burdensome for consumers, as well as being somewhat disingenuous since many consumers are not aware at all of the third party collection of their data on the site.

Two memorandums from the Office of Management and Budget (OMB) provide clear guidance for federal agencies using analytics technology, including those supported by third parties, which in this appears to have been ignored by website developers. According to the OMB’s 2010 “Guidance for Online Use of Web Measurement and Customization Technologies,” web measurement or customization technologies must not “compromise or invade personal privacy.”¹²

¹² Office of Management and Budget. *Memorandum For The Heads Of Executive Departments And Agencies* June 25, 2010. Page 4. “Federal agencies are forbidden from using technologies that: 1) track user individual-level activity on the Internet outside of the website or application from which

The OMB further requires agencies to provide “clear, firm, and unambiguous protection against any uses that would compromise or invade personal privacy.” Additionally, OMB requires that agencies using this technology provide an easy method for the public to opt-out such that the information available to individual users is equal.¹³ The third party sharing practices on HealthCare.gov appears to have violated these guidelines, as it is not clear if, as the agency has stated, turning off cookies would have sufficed to stop this type of sharing.

OMB’s “Guidance for Agency Use of Third-Party Websites and Applications” states “when information is collected through an agency’s use of a third-party website or application, the agency should collect only the information necessary for the proper performance of agency functions and which has personally identifiable information (PII) is collected, the agency should collect only the minimum necessary to accomplish a purpose required by statute, regulation, or executive order.” HealthCare.gov is also in violation of these rules. The government could have chosen to restrict information sharing to only that needed for the functionality of the site, running its analytics internally. Though it’s not clear if the site used retargeting to reach consumers who failed to complete a transaction, it’s dubious whether such a purpose is *necessary* under the OMB guidance.

VI. Recommendations

The privacy and security missteps taken by HealthCare.gov were avoidable. Not only did the OMB offer sound and easy-to-implement guidance on third party sharing scenarios that the website designers ignored completely, there are workable alternatives to third party sharing, such as performing analytics using only first party data collected on HealthCare.gov via software that does not send personal user information to the software maker. Another option would be

the technology originates; 2) share the data obtained through such technologies, without the user’s explicit consent, with other departments or agencies; 3) cross-reference, without the user’s explicit consent, any data gathered from web measurement and customization technologies against PII to determine individual-level online activity; 4) collect PII without the user’s explicit consent in any fashion; or for any like usages so designated by OMB.”

¹³ Office of Management and Budget. *Memorandum For The Heads Of Executive Departments And Agencies* June 25, 2010. Page 5. “Clear Notice and Personal Choice. Agencies must not use web measurement and customization technologies from which it is not easy for the public to opt-out. Agencies should explain in their Privacy Policy the decision to enable web measurement and customization technologies by default or not, thus requiring users to make an opt-out or opt-in decision. Agencies must provide users who decline to opt-in or decide to opt-out with access to information that is comparable to the information available to users who opt-in or decline to opt-out.” “Clear Notice and Personal Choice. Agencies must not use web measurement and customization technologies from which it is not easy for the public to opt-out. Agencies should explain in their Privacy Policy the decision to enable web measurement and customization technologies by default or not, thus requiring users to make an opt-out or opt-in decision. Agencies must provide users who decline to opt-in or decide to opt-out with access to information that is comparable to the information available to users who opt-in or decline to opt-out.”

creating sharing buttons that direct users to social media without sending user information to these sites.

A careful implementation of privacy principles could have prevented the problems with HealthCare.gov. Specifically the site should have used only the data needed for functionality, restricting data sharing with third parties unless absolutely necessary, and adhered to rules that allow for user opt-outs or opt-ins and provide access to information without data sharing. As a general rule, one supported by the recent data breach of Anthem, government agencies and other organizations involved in health information should stop using Social Security Numbers as patient identifiers, encrypt data in transit and at rest, and institute a culture of data privacy and security that includes comprehensive training. We would hope that in the future when a third-party web application or analytics service is installed on HealthCare.gov that 1) at a minimum, a PIA has been conducted and is easily available to visitors via the healthcare.gov privacy policy page; and, 2) that only non-sensitive personal information will be exchanged, intentionally or not, with these third-parties.

The government should address and fix the problems identified in the GAO report. It should also adopt a policy of third party sharing only when necessary for site functionality. It should strictly follow the practical and privacy-protective guidance offered by OMB and should rewrite HealthCare.gov's privacy policy to make it responsive to these recommendations. Ultimately, Congress can best protect consumer information by strengthening legal incentives for companies to better safeguard data and by enacting comprehensive data privacy legislation to give users more insight and control over how their information is collected and used.



KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

Biography of Michelle Kathleen De Mooy
Deputy Director, Consumer Privacy Project
Center for Democracy & Technology

Before the House of Representatives Committee on Science, Space, and Technology,
Subcommittee on Research and Technology, Subcommittee on Oversight

**Can Americans Trust the Privacy and Security of Their Information on
Healthcare.gov?**

February 12, 2015

Michelle De Mooy is Deputy Director, Consumer Privacy Project at the Center for Democracy & Technology. Her work is focused on promoting strong consumer privacy rights through pro-privacy legislation and regulation, working with industry to build and implement good privacy practices, and analyzing emerging privacy concerns. Michelle currently sits on the Advisory Board of the Future of Privacy Forum, a privacy think tank, and has been a panelist and featured speaker at many events related to digital privacy, including Federal Trade Commission workshops, the Internet Governance Forum, Health Privacy Summit, and the State of the Mobile Net.

Prior to CDT, Michelle was Senior Associate, National Priorities at Consumer Action, a national nonprofit focused on empowering underserved and disadvantaged consumers. In this role, she worked extensively with federal agencies, industries, and privacy advocates to build innovative and practical solutions to privacy problems, focusing especially on harms associated with underrepresented communities.

Before Consumer Action, Michelle was a Senior Consultant for eCampaigns at M+R Strategic Services, where she managed online media strategy for the Campaign for Tobacco-Free Kids, The Wilderness Society, and labor rights group American Rights at Work. Michelle provided strategic marketing, communications and technology consulting for non-profits and universities in the Philadelphia area, including the Women's Law Project, Women's Opportunities Resource Center, To Our Children's Future With Health, the University of Pennsylvania and Villanova University.

Michelle was also a senior marketing manager for Investor Broadcast Network where she managed corporate communications, brand advertising and marketing for three web properties, radionwallstreet.com, hedgecall.com, and investorbroadcast.com. She was also involved in the early days of the first dotcom boom, developing software and website projects for startups in San Francisco, including Looksmart, Ltd.

Michelle graduated from Lehigh University in 1997 with a degree in Government.



Chairwoman COMSTOCK. Thank you.
I now recognize Mr. Wright for five minutes.

**TESTIMONY OF MR. MORGAN WRIGHT,
PRINCIPAL, MORGAN WRIGHT, LLC**

Mr. WRIGHT. And it is a pleasure to be in the 10th District. Thank you.

Chairwoman Comstock, Chairman Loudermilk, Ranking Member Lipinski, and Ranking Member Beyer, and Members of the Committee, thank you for inviting me again to testify.

I am Morgan Wright. I am a Principal of Morgan Wright, LLC. I provide advisory and consulting services to the private sector in the area of cybersecurity, advanced technology introduction, strategic planning, and identity theft solutions. In addition, I am currently a Senior Fellow for the Center for Digital Government. The Center is an advisory institute on information technology policies and best practices in state and local government.

Now, I had the honor of testifying before the Committee on November 18, 2013, concerning the security of HealthCare.gov at that time. Since that time, there has been progress made in addressing security and privacy concerns, but yet I find myself repeating many of the same observations today that I made nearly 15 months ago.

I was posed three questions from the Committee. As to the first question, in the healthcare field, there is an approach they call minimum effective dose, which is the lowest dose level that you need to get a significant response. If we apply that to third-party applications on the site, it is apparent to see that out of the 50 previously reported compared to the 11 I observed this morning when I checked the site again, that was an overdose not needed as evidenced by the action of removing 39 of them since discovery. In comparison, Whitehouse.gov and IRS.gov have only four and two third-party applications running respectively. There is no doubt some level of measurement is needed but 50 is digital overkill.

Numerous questions need to be answered by CMS. Are there any written agreements governing the collection and use of PII? How long has each third party been active on the site? How is the use of data governed and audited? Were consumers ever notified that their PII was being shared with third parties? And these are just a few of the questions.

As to the second question, the security of the site has been a primary point of weakness since before the launch on October 1, 2013. In my previous testimony, I highlighted several major issues prior to and after launch. Among them was the lack of and an ability to conduct an end-to-end security test on the production system. The fact that numerous security flaws, flaws that are the most basic type, are left to be discovered by outside third parties, makes it appear HealthCare.gov is crowdsourcing the security and privacy of this important site.

In September of 2014 the GAO issued a report on the site. The highlights state in part that weaknesses remain in both the processes used for managing information security and privacy, as well as the technical implementation of IT security controls. Just some of the key findings: one of the key findings, CMS has not fully implemented security and privacy management controls. It stated

that it did not fully implement actions required by NIST before collecting and maintaining PII.

Another finding: CMS did not document key controls in system security plans. The findings said without complete system security plans, it will be difficult to make a fully informed judgment regarding the risk. Look, if an authorized security decision-maker cannot be fully informed to understand the current risk, it is inconceivable to think that sufficient information exists today to enable 50 third-party applications to operate on HealthCare.gov and to fully understand the associated risk.

Another finding: CMS did not conduct complete security testing. This is an echo of my previous testimony.

And one of the final ones: control weaknesses continue to threaten information and systems supporting HealthCare.gov. And in the finding it said CMS—and this is the troubling one—CMS did not restrict systems supporting the federally facilitated marketplace, FFM, from accessing the internet allowing these systems to access the internet may allow for unauthorized users to access data from the FFM network, increasing the risk that an attacker with access to the FFM could send data to an outside system or that malware could communicate with the command-and-control server.

The unmanaged access to outside connectivity is very disconcerting. The documented activities of Unit 6139A of the Chinese People's Liberation Army and the indictment of five of their members relied upon this exact recipe for their activities. The introduction of third-party applications combined with lack of security, oversight, and control raises the specter of current and undetected state-sponsored penetration of HealthCare.gov. Significant data breaches have been accomplished against far more secure systems.

And as to question three, as NIST continues its leadership role, it has spearheaded the development of the framework for improving critical infrastructure cybersecurity. A review of the framework provides valuable approaches for CMS to utilize in securing the site. The aspect of privacy is so fundamental that it was referred to 30 times in the document. One of the foundational documents is their Special Publication for Information Systems and a key section of the document is Appendix J, Privacy Control. It is a relatively new section but I believe that there is one control under there, AR-3, privacy requirements for contractors and service providers would be applicable in this case to the use of third-party applications and, if followed, would have allowed—would not have allowed for the proliferation of unmanaged data collection.

So thank you for your time and I look forward to your questions.
[The prepared statement of Mr. Wright follows:]

Morgan Wright, Principal - Morgan Wright, LLC

**Testimony of Morgan Wright, Principal, Morgan Wright, LLC,
Before the House Committee on Science, Space, and Technology,
Subcommittee on Research and Technology
and Subcommittee on Oversight**

February 12, 2015

Chairwoman Comstock, Chairman Loudermilk, and members of the Committee:

Thank you for inviting me to testify before you today. I'm Morgan Wright, Principal of Morgan Wright, LLC. I provide advisory and consulting services to the private sector in the areas of cybersecurity, advanced technology introduction, market development, strategic planning and identity theft solutions. In addition, I am also a Senior Fellow for the Center for Digital Government. The Center for Digital Government is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge, and opportunities to help them effectively incorporate new technologies in the 21st century.

I am providing this written testimony pursuant to your invitation to testify. My testimony is in response to the three questions posed by the committee:

1. Why would HealthCare.gov need to embed data mining firms within the website's infrastructure and is it reasonable for there to have been 50 companies connected at one time?
2. What are the cybersecurity implications of the high number of third party connections to HealthCare.gov, and what are the vulnerabilities associated with these types of connections?
3. What guidance does the National Institute of Standards and Technology provide federal agencies relative to cybersecurity practices, and how would they be applicable in this context?

Morgan Wright, Principal - Morgan Wright, LLC

1. Why would HealthCare.gov need to embed data mining firms within the website's infrastructure and is it reasonable for there to have been 50 companies connected at one time?

According to Gartner, data mining¹ is defined as *"The process of discovering meaningful correlations, patterns and trends by sifting through large amounts of data stored in repositories. Data mining employs pattern recognition technologies, as well as statistical and mathematical techniques."*

Investopedia defines data mining² as *"A process used by companies to turn raw data into useful information. By using software to look for patterns in large batches of data, businesses can learn more about their customers and develop more effective marketing strategies as well as increase sales and decrease costs. Data mining depends on effective data collection and warehousing as well as computer processing."*

A reasonable user of the site would be led to believe that there are third-party applications to measure web site statistics, in addition to the obvious social media providers. Since a user coming to the site, either directly or from a referral (like a search engine or link from another site), is not required to enter any personally identifiable information (PII), it is reasonable to assume that their PII later entered on the site would not be passed to anyone other than HealthCare.gov.

The original press reports by AP³ indicated that 50 separate third party applications were collecting data from consumers without their knowledge. According to the story Medicare spokesman Aaron Albright said outside vendors "are prohibited from using information from these tools on HealthCare.gov for their companies' purposes." The use of the term 'vendor' would imply some form of written agreement as to specific prohibitions on use of the data.

¹ <http://www.gartner.com/it-glossary/data-mining>

² <http://www.investopedia.com/terms/d/datamining.asp>

³ http://apnews.myway.com/article/20150120/us--health_overhaul-privacy-8b7c5d925b.html

Morgan Wright, Principal - Morgan Wright, LLC

After the initial report, Cooper Quintin of the Electronic Frontier Foundation published a follow-up article examining the current state.⁴ In it, he wrote “*EFF researchers have independently confirmed that healthcare.gov is sending personal health information to at least 14 third party domains, even if the user has enabled Do Not Track.*” I reviewed the same data on Feb. 10th and observed at least 12 third party sources.

Troubling questions arise as to this practice of allowing numerous companies to access the data, including:

- Does CMS have a standard agreement third parties are required to execute before being allowed access to HealthCare.gov? If so, where are these agreements?
- Does CMS have a list of all companies with third party access? If so, how long has each company been operating on HealthCare.gov?
- If written agreements exist, does CMS verify what data is being collected and that the data is being used only for the specific purpose for which it was collected?
- Does legal counsel review these agreements? What are the specific privacy provisions in each agreement?
- Is data ever sold to third parties? Does CMS charge for access?

The ability to identify a consumer based on their online activity, regardless of the perceived level of anonymity indicated by a privacy policy, was demonstrated by a recent article on a study by MIT scientists and published in the journal Science⁵. The study found that “*Scientists showed they can identify you with more than 90 percent accuracy by looking at just four purchases, three if the price is included -- and this is after companies ‘anonymized’ the transaction records.*”

A consumer visiting HealthCare.gov, providing only minimum information like browser, IP address and operating system could have their ‘anonymous’ data harvested by numerous data brokers, and would be able to match your previous browsing history on other sites and make correlations. While some level of measurement on HealthCare.gov

⁴ <https://www.eff.org/deeplinks/2015/01/healthcare.gov-sends-personal-data>

⁵ http://www.thonline.com/news/business/article_906ceef0-f32f-521f-af2b-06dc8fab74e0.html

Morgan Wright, Principal - Morgan Wright, LLC

is needed (and it makes no business sense not to have any measurement), the use of 50 companies to perform data mining is digital overkill and puts the PII of consumers at significant risk.

2. What are the cybersecurity implications of the high number of third party connections to HealthCare.gov, and what are the vulnerabilities associated with these types of connections?

The security of HealthCare.gov has been a primary point of weakness since before the site launched Oct. 1, 2013. In my previous testimony before the House Science, Space and Technology Committee on November 18, 2013, I highlighted several major issues prior to and after launch. Primary among them was the “...lack of, and inability to conduct, an end-to-end security test on the production system. The number of contractors and absence of an apparent overall security lead indicates no one was in possession of a comprehensive, top-down view of the full security posture.”

The fact that numerous security flaws, flaws that are the most basic type (unencrypted PII, SQL injection attacks, etc.) are left to be discovered by outside third parties makes it appear HealthCare.gov is crowdsourcing the security and privacy of the site.

In September of 2014, the United States Government Accountability Office (GAO) issued a report entitled “HEALTHCARE.GOV – Actions Needed to Address Weaknesses in Information Security and Privacy Controls”. (GAO report, GAO-14-730⁶) The highlights clearly state that “ *While CMS has taken steps to protect the security and privacy of data processed and maintained by the complex set of systems and interconnections that support Healthcare.gov, weaknesses remain both in the processes used for managing information security and privacy as well as the technical implementation of IT security controls*”.⁷

⁶ <http://www.gao.gov/products/GAO-14-730>

⁷ <http://www.gao.gov/assets/670/665841.pdf>

Morgan Wright, Principal - Morgan Wright, LLC

There are several key findings worth noting and expounding upon. In this section, I will outline those findings and provide a high-level observation of the cybersecurity implications for each. It must be noted that privacy and security are intertwined – you cannot have one without the other. Policies are only as effective as the implementation, enforcement, management, audit and revision of them.

Information Security and Privacy Weaknesses Place Healthcare.gov Data at Risk (Page 35)

“However, CMS has not fully addressed security and privacy management weaknesses, including having incomplete security plans and privacy documentation, conducting incomplete security tests...”

In my original testimony, this was a key area I highlighted that was critical and needed immediate resolution to. It is a known maxim that you cannot manage what you cannot measure. CMS is unable to measure the security of HealthCare.gov because it has never successfully completed comprehensive security testing of the entire site. Adding third-party applications without proper due diligence and compliance speaks to the continued lack of oversight and management of the security of the site. Willfully or unintentionally ignoring established governance mechanisms and security controls in order to add up to 50 third-party applications is incomprehensible.

CMS Has Not Fully Implemented Security and Privacy Management Controls Associated With Healthcare.gov (Page 42)

*“Though CMS developed and documented security policies and procedures, it did not fully implement actions required by NIST **before** (emphasis added) Healthcare.gov began collecting and maintaining PII from individual applicants.”*

The failure to follow published, documented and widely available security guidance from NIST, even when compliance was mandatory, only increases the likelihood of a preventable security incident. Because privacy controls were not fully implemented, it is difficult to understand how CMS and HealthCare.gov could truly understand the scope

Morgan Wright, Principal - Morgan Wright, LLC

and magnitude of any Personally Identifiable Information (PII) being collected and used by third party applications – **especially applications that are data mining products**. And, because security controls were also not fully implemented, it is just as difficult to understand how CMS prevented unauthorized access to, or use of, this PII.

CMS did not document key controls in system security plans (Page 42-43)

“Without complete system security plans, it will be difficult for agency officials to make a fully informed judgment regarding the risks involved in operating those systems, increasing the risk that the confidentiality, integrity, or availability of the system could be compromised.”

This finding was written months before the existence of the 50 embedded third party applications that spawned the current hearing before the Committee. If an authorized security decision maker cannot be fully informed in order to understand the current risk, it is inconceivable to think sufficient information exists to enable 50 third party applications to operate on HealthCare.gov and to **fully understand** the associated risks.

CMS did not fully assess privacy risks in PIAs (Page 43)

“CMS privacy documentation was also incomplete. OMB requires agencies to assess privacy risks as part of the process of developing a privacy impact assessment (PIA)... However, in completing these PIAs, CMS did not assess the risks associated with the handling of PII or identify mitigating controls to address such risks.”

Given the amount of time the system has been under development, and the amount of money spent, the one area CMS should have excelled at is privacy. The failure to fully understand and document the privacy impacts only means future decisions will also be based on incomplete information, as in the case of the third party applications.

Morgan Wright, Principal - Morgan Wright, LLC

CMS did not conduct complete security testing (Page 46)

“NIST and CMS guidance make clear that the security of complex systems such as the FFM and interconnected systems needs to be tested in a comprehensive fashion that takes into consideration how the systems are interconnected and how security controls are managed across all interconnected systems...”

(Page 49) “Without comprehensive testing, CMS does not have reasonable assurance that its security controls for the FFM are working as intended, increasing the risk that attackers could compromise the confidentiality, integrity or availability of the system.”

Unless, and until, CMS is able to conduct a complete security test, it will forever be unable to make a qualified risk decision relating to privacy and security. This means avoidable risks will become unavoidable, and preventable incidents will become unpreventable.

A primary source of this risk was the apparent unabated installation of third party applications that collected numerous types of data from consumers visiting HealthCare.gov – data they were unaware of that was being collected and not informed of prior to. It cannot be underscored heavily enough that a fundamental task CMS should do, without further delay, is the complete end-to-end security testing of HealthCare.gov.

Control Weaknesses Continue to Threaten Information and Systems Supporting Healthcare.gov (Page 50)

(Page 51) “CMS did not effectively implement or securely configure key security tools and devices on the systems supporting HealthCare.gov to sufficiently protect the users and information on the system from threats to confidentiality, integrity and availability.”

Morgan Wright, Principal - Morgan Wright, LLC

“CMS did not restrict systems supporting the FFM from accessing the Internet... Allowing these systems to access the Internet may allow for unauthorized users to access data from the FFM network, increasing the risk that an attacker with access to the FFM could send data to an outside system, or that malware could communicate with a command and control server.”

The key word in the finding is “continue”. Consumers using HealthCare.gov are exposed to ongoing risk that their PII will be compromised, or used inappropriately by third party applications. Most troubling is the finding that these systems had access to the Internet. The unmanaged access to outside connectivity is very disconcerting. The documented activities of Unit 61398 of the Chinese PLA, and the indictment of four of their members, relied upon this exact recipe for their activities.

The introduction of third party applications, combined with lack of security oversight and controls, raises the specter of current undetected state-sponsored penetration of HealthCare.gov. Significant data breaches have been accomplished against far more secure systems.

3. What guidance does the National Institute of Standards and Technology provide federal agencies relative to cybersecurity practices, and how would they be applicable in this context?

Throughout the GAO report, numerous references to NIST publications are documented. As NIST continues its leadership role, it has spearheaded the development of The Framework for Improving Critical Infrastructure Cybersecurity⁸ (The Framework). This was authorized by on February 12, 2014, via Executive Order 13636.

In addition, NIST has also developed the *Risk Management Framework*⁹ that has marshaled all of the Federal Information Security Management Act (FISMA) standards

⁸ <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>

⁹ <http://csrc.nist.gov/groups/SMA/fisma/framework.html>

Morgan Wright, Principal - Morgan Wright, LLC

and guidance in order to generate the proper awareness and development of comprehensive security programs.

The Framework

A review of The Framework provides valuable approaches for CMS to utilize in securing HealthCare.gov. Through the Executive Order, the issues of security and privacy were specifically addressed. The Order states *“It is the Policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.”*

The aspect of privacy is so fundamental to The Framework, it is mentioned over 30 times in the document. The other aspect that makes The Framework a model approach is the voluntary collaboration between the public and private sector in developing the document. While it is voluntary, the benefit of the collective insight and experience across multiple sectors and domains is impressive.

The Framework is a collection of 97 controls and 5 discrete functions. The functions contain relevant categories and subcategories for each function, along with a set of informative references for each subcategory. The advantage of The Framework over FISMA is that The Framework is a living document – constantly updating and evolving based on the collective contributions of all.

One of the foundational documents of The Framework is NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (includes updates as of Jan. 15, 2014)¹⁰. SP 800-53 Revision 4 is a furtherance of the statutory responsibilities of NIST under FISMA.

¹⁰ <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

Morgan Wright, Principal - Morgan Wright, LLC

A key section of SP 800-53 Revision 4 is Appendix J – *Privacy Control Catalog*. It is a relatively new section intended to “address the privacy needs of federal agencies”. According to the document, the Privacy Appendix addresses some of the key issues, such as:

- Provides a structured set of privacy controls, based on best practices...
- Establishes a linkage and relationship between privacy and security controls...
- Demonstrates the applicability of the NIST Risk Management Framework...
- Promotes closer cooperation between privacy and security officials...

Under Appendix J, there is a set of controls that belong to the ‘Accountability, Audit and Risk Management’ family. I believe control ‘AR-3 Privacy Requirements For Contractors And Service Providers’ would be applicable to the use of third party applications. And, if followed, would not have allowed for the proliferation of unmanaged data collection. In part, the control says:

- a. *Establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and*
- b. *Includes privacy requirements in contracts and other acquisition-related documents.*

Supplemental Guidance: *Contractors and service providers include, **but are not limited to** (emphasis added), information providers, information processors, and other organizations providing information system development, information technology services, and **other outsourced applications** (emphasis added). Organizations consult with legal counsel, the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), and contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control.*

The foregoing is in addition to the security controls in Appendix F (*Security Control Catalog*) and G (*Information Security Programs*). The application of this one control could have mitigated the unnecessary exposure of PII by HealthCare.gov.

Morgan Wright, Principal - Morgan Wright, LLC

Morgan Wright's professional career includes over 17 years of service in state and local law enforcement as a city officer, state trooper and detective. He provided in-service training to the FBI Computer Analysis Response Team (CART) Team on the investigation of computer intrusions. Morgan was also an instructor for the US State Department, Diplomatic Security Service, Antiterrorism Assistance Program. He delivered briefings on cyberterrorism in Pakistan and Turkey.

Over the last 15 years, Morgan has held positions in companies who specialized in systems integration, defense, intelligence, justice, consulting, network and information security, advanced technology and broadband communications. His subject matter expertise was used for several programs, including Technology Exploration Development, Counterintelligence Field Activity; Consolidation of The Terrorist Watch Lists, and; Concept of Operations – Law Enforcement Information Sharing Program (LEISP), Department of Justice (now called OneDOJ).

Morgan's technology leadership includes Global Industry Solutions Manager at Cisco for Public Safety and Homeland Security. He later become the Vice President of Global Public Safety, End-To-End LTE, at Alcatel-Lucent, delivering the first deployment of a secure, public safety broadband network, now the mission of FirstNet.

In 2012 Morgan served as the Senior Law Enforcement Advisor at the Republican National Convention, deploying a secure, private broadband network. He currently is the Principal at Morgan Wright, LLC providing advisory and consulting services to the private sector in the areas of cybersecurity and identity theft solutions. He is also a Senior Fellow for the Center for Digital Government, a national research and advisory institute on information technology policies and best practices in state and local government.

Morgan is the author of two chapters in the 4th Edition Computer Security Handbook, and holds bachelor's degrees in Computer Information Systems and Human Resource Management. He is a 2011 graduate of the Executive Leadership and Management Program, Mendoza College of Business, University of Notre Dame.

Morgan Wright, Principal - Morgan Wright, LLC

Morgan Wright's professional career includes over 17 years of service in state and local law enforcement as a city officer, state trooper and detective. He provided in-service training to the FBI Computer Analysis Response Team (CART) Team on the investigation of computer intrusions. Morgan was also an instructor for the US State Department, Diplomatic Security Service, Antiterrorism Assistance Program. He delivered briefings on cyberterrorism in Pakistan and Turkey.

Over the last 15 years, Morgan has held positions in companies who specialized in systems integration, defense, intelligence, justice, consulting, network and information security, advanced technology and broadband communications. His subject matter expertise was used for several programs, including Technology Exploration Development, Counterintelligence Field Activity; Consolidation of The Terrorist Watch Lists, and; Concept of Operations –Law Enforcement Information Sharing Program (LEISP), Department of Justice (now called OneDOJ).

Morgan's technology leadership includes Global Industry Solutions Manager at Cisco for Public Safety and Homeland Security. He later become the Vice President of Global Public Safety, End-To-End LTE, at Alcatel-Lucent, delivering the first deployment of a secure, public safety broadband network, now the mission of FirstNet.

In 2012 Morgan served as the Senior Law Enforcement Advisor at the Republican National Convention, deploying a secure, private broadband network. He currently is the Principal at Morgan Wright, LLC providing advisory and consulting services to the private sector in the areas of cybersecurity and identity theft solutions. He is also a Senior Fellow for the Center for Digital Government, a national research and advisory institute on information technology policies and best practices in state and local government.

Morgan is the author of two chapters in the 4th Edition Computer Security Handbook, and bachelor's degrees in Computer Information Systems and Human Resource Management. He is a 2011 graduate of the Executive Leadership and Management Program, Mendoza College of Business, University of Notre Dame.

Chairwoman COMSTOCK. Thank you very much. I thank the witnesses for their testimony and insights.

And now we are going to do questioning for five-minute rounds. And I will recognize myself for five minutes.

Now, given that we first learned about these I guess about three weeks ago. If we were—and this is to both of you—if HealthCare.gov were employing a lot of the management tools that you have outlined here for us, would CMS be able to fairly simply tell us what was going on? Is it something that should take a long time for them to tell what their system does and whether it is safe or not? Because I think from the consumers' standpoint, I think we would like to know pretty quickly what is going on one way or the other in case it needs to be remedied, like you said in the case of if 50 is too many, what is okay or what is—shouldn't they know how many are there? So I am just trying to get a sense of what should they be doing so that they can tell us something fairly basic like this pretty quickly.

Mr. WRIGHT. You bring up—and I appreciate the question. You bring up from my prior testimony, I think one of the fundamental things that has to be done is a complete end-to-end security test of the production system. It is referenced again in the GAO report and Ranking Member Lipinski, even to your comments, there has been a lot of significant progress made. They do need to do marketing but we all want that marketing to be safe. You know, HealthCare.gov isn't about R's and D's. It is about ones and zeros. It has no allegiance to a party. It does what it is told and my concern is that the ones and zeros are not being told to do the right things to protect not only the privacy but the security. You can't have total visibility of a system until you understand end-to-end. And the government would not allow a car to be sold on the open market unless it went through a complete crash test. You cannot test individual components of a car and say it is safe; it has to go through the entire gambit. And HealthCare.gov should do the same.

Ms. DE MOOY. Yes, thank you for the question. I think from a consumer perspective the way that people would have found out about this was through the privacy policy, and we found a lot of problems with the HealthCare.gov privacy policy. For example, it is very broad and very vague. They don't define personally identifiable information and there are guidelines in NIST for defining this, but the impetus is on the privacy policy to sort of define it for itself so that there aren't any loopholes in which data can fall through. So that would have been very helpful. That would have been a form of transparency that would have allowed people to understand a little bit more.

Also, the privacy policy kind of deferred to the privacy policies of the third parties. So it was—the onus was on the consumers or the visitors of the site to find out the policies then of the third parties, which is a little disingenuous considering that many of people had no idea that these third parties were there in the first place.

Chairwoman COMSTOCK. You know, if one of the reasons why they are doing this is they are trying to reach more people to say hey, you might be eligible, you know, whatever you are doing, aren't there other much safer ways to do that? Like, say, you know,

if we know a particular ZIP code has a high density of uninsured people, you can—I mean would it expose anyone’s privacy if you were maybe advertising online to somebody in their ZIP code or, you know, you were doing outreach efforts that are targeted to targeted populations? Is there a way—what is the best—you know, sort of best practices on doing that in a way that secures people’s privacy?

Ms. DE MOOY. Sure. Yes, Chairwoman, I think that the way that you put it is exactly right, that there are ways to limit it to certain data points so that you are not getting unnecessary data in order to do things like retargeting. And yes, there are very good reasons why the government, to fulfill its mandate, would need to do outreach to try to get more enrollment, to try to get people aware of these programs.

That said, I think the way that my fellow witness here put it, it was overkill. There was no need for the leakage that occurred. And I think some of this is governed by the contracts that existed between the government and the vendors that they used, and I think it would be very helpful for when the government witnesses are here to find out exactly what the terms of those contracts were in terms of data sharing.

Mr. WRIGHT. Just a quick follow-up, too. You know, I am not the marketing expert, but however, I do know is that a great marketing product or software implemented poorly is still a poorly designed product. And the concern is is that even though as these things collected data and information, there is a huge issue with the collection of data by several—there are about 52 major data brokers that, if you want to find out what somebody is doing online, their address, we saw this in Ferguson, we saw this with ISIS and the compromise of the CENTCOM site. They are using personally identifiable information to target people.

Ask Colonel Replogle of Missouri Highway Patrol. His information was released by Anonymous and he was specifically targeted. So these things—these programs have consequences if not managed correctly.

Chairwoman COMSTOCK. Thank you very much.

And I now recognize Mr. Lipinski.

Mr. LIPINSKI. Thank you, Madam Chairwoman.

I just want to make sure we try to take a couple steps back here because there is a lot we don’t know unfortunately. And I do look forward to asking questions of the—of the CMS.

But just so I have a better understanding, I think we discussed the use of third-party analytics tools is common in both private and governmental websites. What usually is done on a private website when they are using a third-party data analytic—how is it—how is privacy—and again, we have to talk about what the standards are going to be, but what is usually done? When I go to a website, how often are there third parties looking at the data and what happens with that and how do I know that there are third parties? What is going on with that and am I—is there any way that I am protected if I am going to a private website?

Ms. DE MOOY. Thank you for the question. It is a great question and is sort of begins at the layers of communication that occur when you go onto the web. Some of them are behind the scenes and

some of them are more apparent. It is rampant on the web certainly with commercial websites but even, you know, all sorts of entities. Data sharing is absolutely aggressive. So in terms of protections, there are very few. There are settings that you can place on browsers that restrict or at least broadcast the fact that you would not like to be tracked, but those are sort of on the honor system right now, which makes it difficult to enforce.

But just to get back to your technical question, when you are online and say, for example, you click on a link or you go to a website, it will trigger a message from your browser to the intended website's server and that sort of announces your arrival to them and it will share basic information about you like your IP address, which I think most people know but it is sort of like your telephone number is your address on the telephone network. Your IP address is your address on the internet. And the information exchanged usually during this point is just utilitarian, sort of what does your browser support so that the website will load correctly?

When a website wants to customize this and wants to sort of remember who you are and remember certain places that you may have gone, things you are interested in, which is how we put customization, they may enact third parties and that may involve dropping a cookie, which is sort of a little recorder is the way I like to think of it, onto your computer and that will observe where you have been and it will also observe where you are going to, so different websites the you are surfing to. And if the site wants to do marketing and advertising, they will employ third parties and they will have different contracts. And this can be up into the hundreds and thousands for some sites.

Mr. LIPINSKI. And why would there be so many?

Ms. DE MOOY. Well, it is a lucrative business and data miners and advertising networks work in real time, and so the time that you are online may feel slow to you but to the advertising networks, they are grabbing millions and trillions of data points every single second. And so that is monetized then into serving advertisements. So the more, the merrier.

Mr. LIPINSKI. Okay. Because is there any—the question is for the—for HealthCare.gov is why were there so many—however many it is—and we are still not exactly sure how many—why would there be a dozen, two dozen, three dozen—

Ms. DE MOOY. Um-hum.

Mr. LIPINSKI. —and why would HealthCare.gov—why would they use that many?

Ms. DE MOOY. To me that is inexplicable to be quite honest. I can tell you that the rationale would probably include web customization, so wanting, as they said, to make the site more streamlined, more intuitive for people so that it is easier to find access to the information they are looking for. In other words, if a consumer comes to a website and they really just want to see the plan rates, but the website will serve that to them the next time and it sort of remembers that.

The act of having—especially for a government website—that many entities in order to do something like retargeting to me is inexplicable. I think it is an example—and this is just speculation—is an example of when you have multiple different contractors

working on a project, this was sort of the easiest and kind of laziest way to design the site, to do—there are ways to do it in-house and there are ways to do it in a more privacy-protective manner, but that was not done here.

Mr. LIPINSKI. Okay. There are ways to do that in-house, you said—

Ms. DE MOOY. Yes.

Mr. LIPINSKI. —and your testimony you had talked about that. I think I am going to—my time is almost up. I want to make sure everyone else has questions.

If we have time for a second round, I will have more, but I yield back.

Chairwoman COMSTOCK. Thank you.

I now recognize Mr. Johnson five minutes.

Mr. JOHNSON. Thank you, Madam Chairman. And thank you to the panelists for being here today.

I can tell you that as a 30-plus year IT professional both in the Department of Defense and in the private sector I remain very, very concerned about the inadequacy of security and the safeguarding of consumers', hard-working taxpayers' personal private information.

Ms. De Mooy, in May of 2013 the President issued that Executive Order to establish an open data policy to make open and machine-readable data the new default for government information taking really historic steps to make government-held data more accessible to the public and to entrepreneurs while appropriately safeguarding sensitive information and rigorously protecting privacy, or so it is stated.

Let's go back for a second so that I can get this straight. Is it mandated in your opinion—it has been mandated by the government that Americans need to sign up for healthcare and that, for the most part, they will do so on the government-created website HealthCare.gov, correct?

Ms. DE MOOY. That is correct—

Mr. JOHNSON. Okay.

Ms. DE MOOY. —as far as I know.

Mr. JOHNSON. Now, once they are on HealthCare.gov, they have to give their personal information in order to sign up for their healthcare, correct?

Ms. DE MOOY. That is correct, sir.

Mr. JOHNSON. Okay. And with what we are learning today, the government is then helping companies through this Open Data Initiative to collect all of that personal information of the American people—on the American people, correct?

Ms. DE MOOY. I am not quite sure what the question was.

Mr. JOHNSON. What we have learned from the President's Executive Order and all of this open data transformation that he has done, we are learning that the government is helping these outside companies through their data mining efforts, through this Open Data Initiative to collect all of that personal information on the American people, correct?

Ms. DE MOOY. My understanding of the Open Data Initiative is a bit different. It is more about actionable data that can be used to help the public or for the public. It is more about transparency.

And in this case, transparency would have been very helpful. I think that the fact that people have no choice when they come is a serious problem that should have held the government to a higher standard in terms of protecting their privacy and security.

Mr. JOHNSON. Well, again going back in my experience and something that Mr. Wright said a little earlier, you know, this is not rocket science. It is ones and zeros. And if they are allowing this Open Data Initiative to collect some information that is out there, I mean we have seen how many different commercial and government systems have been hacked by the bad guys already—

Ms. DE MOOY. Um-hum.

Mr. JOHNSON. —and with the security concerns that we have got about HealthCare.gov already, do you believe that the Administration is yearning for greater openness to make government-held data more accessible? Do you believe that has, whether intentionally or unintentionally, potentially compromised American citizens' privacy on HealthCare.gov?

Ms. DE MOOY. In my opinion, no. I think the government—I can't speak for what the intentions were. I don't have any direct knowledge of that, but I can say that my understanding of the Open Data Initiative was about giving citizens more opportunities for actionable data, more transparency in the government, and I think in this case it had more to do with the function of the site, which was to reach as many people as possible, to, you know, do some advertising and marketing to get to the populations that would be interested in this. And I think they went far beyond what was necessary and far beyond what their own government has suggested and prescribed.

Mr. JOHNSON. I am running out of time.

Mr. Wright, same question to you. Do you think that allowing this Open Data Initiative, have we potentially compromised American citizens' privacy on HealthCare.gov given what we already know about the security inadequacies of the system?

Mr. WRIGHT. My opinion would be yes because it is a—because now what you are mandating is a philosophy and a direction to say everything will be shared except for maybe some certain things. So people may be interpreting what the intent of the Executive Order was and they are attempting to do things, but without clear guidance, without clear structure, without clear privacy and security, you then get the law of unintended consequences, which is the information is used improperly and collected improperly and collected in an unabated fashion.

Mr. JOHNSON. I tend to agree with you, Mr. Wright. I respect your opinion, Ms. De Mooy, but as someone who has had to provide security to systems—in systems, I personally think we have opened the proverbial barn door and the cows are going to get out. And with that, I—my time is expired.

Ms. DE MOOY. I am sorry. I just had one additional comment to make, sir.

Just—I think The Open Data Initiative should be coupled with the understanding that trust is necessary. The people needed to have trust in the systems and particularly when it comes to healthcare Americans shouldn't have to choose between privacy and health.

Mr. JOHNSON. Oh, my goodness, Madam Chair, you are exactly right. The people should be able to trust, but the Administration has demonstrated clearly that it is not a trustworthy system.

Ms. DE MOOY. Right, and perhaps proverbial—

Mr. JOHNSON. Security was never designed into the system in the first place.

Chairwoman COMSTOCK. Thank you.

I now recognize Mr. Beyer for five minutes.

Mr. BEYER. Thank you, Madam Chair.

Mr. Wright, I just wanted to clarify one thing. You suggest in your testimony that personally identifiable information was released from HealthCare.gov and it is true that information was released to third parties—we have heard about this, the 50 people—50 agencies, and there certainly are legitimate privacy-related questions, but from everything I know there is no PII data that was actually released and certainly no medical records.

Unfortunately, we have seen many, many other instances of PII data released on a frequent basis. Last year, eBay revealed that hackers had stolen the personal records of 233 million users, including usernames, passwords, phone numbers, and physical addresses. Anthem, we talked about, with the 80 million. My wife seems to get a new credit card every 90 days because the bank sends her a note saying the credit card has been compromised. And these are all unfortunate circumstances but they point to larger issues, security and privacy, but I don't think they point to specific PII data from HealthCare.gov. Your comments?

Mr. WRIGHT. No, correct. And it is not the implication that people's complete PII was released, but when you take pieces of information such as your age, your income, whether you are pregnant or not or you smoke, the whole point about the ability to correlate from large amounts of data sets, your visit at HealthCare.gov combined with information from other data brokers or other things that you have done has now created the opportunity, and actually the end result then is the disclosure because you provided the key components that link behavior on one side or behavior on the internet now to very specific information about you.

The Chair, when she released her statement, is one of the things in my written testimony about MIT. We have now gotten to the point on the internet to where there is so much data floating out there it takes very small steps to be able to create a profile on user to understand where you live, what you do, what your interests are. Marketers use it all the time but the issue—the difference between the public sector and the private sector is if my information gets exposed from eBay, there will be 1,000 attorneys filing class-action lawsuits. Unfortunately, with the immunity of the federal government, citizens don't have the same recourse. So to your point, that higher standard needs to be there. So because I don't have that recourse I should then have the higher standard to not have to worry about that.

But in total agreement, no specific PII was released, but the combination of factors and bringing it all together, it is the totality of the circumstances, not an individual action.

Mr. BEYER. Okay. Thank you very much.

Ms. De Mooy, is there any reason not to prohibit third-party vendors and can the website even be evolved to work without outside vendors, in-house data analytics? And I wonder, too, this is very speculative, but we know how tortured the rollout of HealthCare.gov was. How much of this do you think was the crashing and burning of CGI and the replacing with Accenture and all the firms trying to put Humpty Dumpty back together again?

Ms. DE MOOY. Well, I appreciate that analogy. I don't have any knowledge about the mechanisms that went on. I can speculate that when you hire a lot of outside vendors to work on one project, that the communications can fall apart. And I think in this case, when I look at the site design, it feels to me a bit lazy. And like I said before, the easiest thing is to just allow rampant sharing. It is a little more technical and in fact more well-designed to limit that sharing.

Yes, the government could do some of the analytics, definitely the analytics in-house. They could create sharing buttons. They could have, you know, really ironclad privacy policy that includes privacy policies for their third parties as opposed to sort of adopting the policies of their third parties.

Mr. BEYER. You had mentioned that we need comprehensive data privacy legislation.

Ms. DE MOOY. Correct.

Mr. BEYER. Is there such model legislation out there?

Ms. DE MOOY. We are waiting on the White House. They had said that they would release it 45 days after the President's State of the Union address.

Mr. BEYER. Okay. Great. Thank you.

I yield back, Madam Chair.

Mr. WRIGHT. Could I actually add just one comment? Is that okay?

To your point, though, actually I think one of the things that would help is really not a technical issue. Back in my day doing work inside the justice, the intelligence community, the one thing that always had to be there was that executive sponsorship, that single point of contact who is what—we used to call it the single throat to choke. I think something that would vastly help and I think the implementation of Accenture over CGI, bringing in people who actually have the ability to do that leadership and create that single point of leadership. I think that is one of the biggest failures is there was no single prime in charge of the entire project. We had a lot of stovepipes, which we know from information sharing caused problems. I think the biggest thing they could do is really get down to that single point of contact, who is the true leader that I can go to, push their belly button, and solve all of my problems?

Mr. BEYER. Thank you very much.

Chairwoman COMSTOCK. Good. I now recognize Mr. Posey for five minutes.

Mr. POSEY. Thank you, Madam Chairman.

I understand the purpose of retargeting. When I look at a barbecue or a bathroom vanity or a power tool on a hardware store website, I understand, but it doesn't necessarily make me comfortable that the same product pops up on the next website that I

visit. And, you know, I understand the idea that companies want to be able to target me in a similar way, but I don't understand why HealthCare.gov would feel the need to have such similar tactics incorporated as to hardware store or Zappos or whatever. I mean it seems like a larger invasion of privacy. It seems like a larger invasion of privacy to me. Just wondering what your thoughts are, both of you?

Ms. DE MOOY. Thank you for the question. I think the reason that I would imagine that the government would give for doing re-targeting, which, as I said before, it isn't certain—it appears to be likely but it is uncertain—the reason they would have done that would be to find the people who needed the information, so to reach into communities where people who don't have health insurance live, go to the sites, and the way that they would learn this is by, you know, sharing the information and learning where people come from to where they first learned about it and link to the site and go and making sure that they are advertising at that site.

One of the problems with that in terms of—from a privacy advocacy perspective is that when you reach into communities such as those that don't have health insurance, you are often reaching into communities that are disadvantaged, and there have been studies and surveys that show that people who are disadvantaged tend to suffer more privacy harms in terms of being labeled. I know the Senate Commerce Committee report came out that identified some of these labels has “urban and barely making it,” “second city ethnic,” things that are insulting to say the least but also can actually accelerate the cycle of poverty by sending things like predatory loans and different sorts of interest rates.

Mr. WRIGHT. I am with you. I confuse privacy and property all the time. I think I buy too much online sometimes.

My aspect on it though is not from a marketing standpoint, but any time—if you take a penny and you double it, you know, every day for 31 days, you end up with \$10,700,000. Every time you add another component, every time you add more things that have to be done, every time you add another third-party application, you just don't arithmetically increase the attack vectors; you geometrically increase all the things you have to defend against.

That is why in my opening statement I talked about, you know, physician, heal thyself. Use a minimally effective dose. Use only the things you need to use to accomplish the mission you need to accomplish. It should be a well-defined business case that has security and privacy impacts understood before you do it, and then when you get things like re-targeting and stuff, then you have very limited scope specifically addressed. But to my—from my perspective, you limit the vulnerabilities then to the site and the amount of things that can be exploited because one program of itself may be secure, but combined with another one and a third one could create a host of unintended vulnerabilities you are not aware of because you have never tested that combination of programs before.

Mr. POSEY. Thank you. And good answers.

Is there a requirement or standard or practice for private companies to inform visitors about third-party analytics?

Ms. DE MOOY. Yes, sir. Generally, this is done through a privacy policy, which I would imagine most of us in here don't read. I know

that I have been guilty of that. They are very lengthy usually in sort of a legalese that is difficult for most people to wade through. So we almost always agree if it is something that preempts joining a service or a site.

The government in this case should be held to a higher standard than that in my opinion not just because the government should be the steward of privacy and security but also because, as I said, people don't have a choice. They need to go to this website and they should have been given a choice about whether to share their data.

Mr. POSEY. Mr. Wright?

Mr. WRIGHT. And actually just one point, I mean do you know how many companies would pay big dollars to guarantee 10 million visitors to their site? I mean it is—there is a—that is, you are right, big money, and there is no choice for them to go to that. And so to that point it does need to be a higher standard because they don't have a choice. Consumers have a choice of going to private websites. They also have the choice of litigation. So with Anthem, with eBay, with all the other ones, there will be litigation over this but is very difficult to sue the federal government.

Mr. POSEY. Very good.

Thank you, Madam Chair. I yield back.

Chairwoman COMSTOCK. Thank you.

I now recognize Ms. Bonamici for five minutes.

Ms. BONAMICI. Thank you very much, Chair Comstock and Ranking Member Lipinski.

This has been a very interesting discussion, and I have to say that it really highlights the issues of—two issues of importance: access to healthcare and protection of personal privacy. I spent part of this morning in a hearing in the Education Committee about privacy regarding student records, and I said then and will say again that whenever we are talking about legislating in the area of technology, it is always a challenge to find the right balance because, as we all know, the technology advances usually a lot quicker than the legislation so we want to make sure that we are finding the balance that protects people's privacy but does not inhibit valid, useful purposes for technology and advances in technology.

So I really do look forward to hearing from CMS and hearing their answers. I know we have had some hearings on this issue before but highlighting from them. As Ranking Member Beyer said, it would have been best to have them answer questions first and then we could follow up on what they said.

But, you know, I want to say that we all acknowledge that there are legitimate problems with HealthCare.gov. Certainly in my State of Oregon we did not do a good job at all with that. But it is also important to remember that the Affordable Care Act is about more than a website; it is about access to healthcare for millions of Americans.

I want to make sure that we don't, in this hearing and other hearings in the future, spread any sort of unfounded fear or misinformation when really our constituents are looking for clarity. So I hope we can help inform them about ways that they can protect their privacy online and specifically keep their personal information safe.

And I want to ask you, Ms. De Mooy, and follow up on the conversation you were having with Mr. Posey, that you say in your testimony that consumers from disadvantaged communities face more potential harm such as being profiled in databanks. So given the importance of the Affordable Care Act to disadvantaged communities that have historically lacked access to affordable healthcare, how can HealthCare.gov do a better job of serving those consumers while also protecting their privacy?

Ms. DE MOOY. Thank you so much for the question.

The government needs to implement the recommendations that I outlined my testimony that include guidance from OMB that really lays out exactly how a government should interact with third parties. It is very privacy-protective. It is also practical in terms of using sharing technologies, using web analytics technologies.

And also my fellow witness brought up and I should mention the GAO report in 2014, which appears to have been ignored. I am not sure exactly if that is the truth, and it would be really good to hear from the Administration on the progress, but those are also excellent privacy and security guidances that the report gave. So I would say that that would be a good start. And it is actually—as opposed to a data breach, it is something the government can do right now.

Ms. BONAMICI. Right. And I look forward to following up on that when the Administration is here.

So we talked a lot about the personally identifiable information, or the PII, and I am just intrigued by this whole discussion because, you know, we—Mr. Posey was talking about Zappos and shopping online and how he gets those ads, and not to minimize the issue, but say, for example, someone is searching for a cure for morning sickness or newborn clothes, might someone figure out that perhaps they were pregnant? Or what if they shopped for some sort of product to quit smoking? My point is that there are a lot of ways that I guess these third party companies can figure out those personal—personally identifiable issues.

So just to confirm, has any personally identifiable information been gathered through HealthCare.gov—been used improperly?

Mr. WRIGHT. You bring up a very good question. By the way, sorry about the Ducks. They beat Florida State, Notre Dame—

Ms. BONAMICI. Oh, I was—

Mr. WRIGHT. —so I am with you on that.

Ms. BONAMICI. Sorry you reminded me about that, though. I am still recovering.

Mr. WRIGHT. Yeah. The issue is—and I go back to it—it is the GAO report. It is what I said November 18, 2013. They have never done an end-to-end security test, so until you do, you do not know that PII has never been exposed. All you can say is as far as we know, which back in my days as a detective always got me in trouble with the defense attorneys, as far as I know, so you don't know everything, you just know that.

Ms. BONAMICI. Yeah, and I understand that they did an end-to-end security review in December and they are currently reviewing that, so we will make sure that we ask about that when—

Mr. WRIGHT. Well, actually it was a review of controls as opposed to an end-to-end full system security test of the production system.

Ms. BONAMICI. Thank you. And I do want to try to squeeze a question in—

Mr. WRIGHT. Sure.

Ms. BONAMICI. —in the last couple seconds about human factors, research, and I know that—I mean, Ms. De Mooy, you talked about how people just tend to click without reading policies. They are given to following what is convenient, don't understand the fine print or the options, so is there some research that we can do or that can be done that will help inform consumers so that they can better protect their privacy and defend against cybersecurity threats? Is there certain kinds of research that we need to help our consumers and constituents?

Ms. DE MOOY. Honestly, no. There have quite a few reports and studies done and I think almost every aspect of this has been looked at and picked apart either by academics or technologists or advocates. I think simply entities, government entities, commercial entities, need to take privacy insecurities very seriously and not view the opportunities to get data as, "I will collect as much as I can and then figure out what to do with it later," but to have very solid systems in place that include privacy risk assessments and privacy model threats, which is, you know, something that is a sort of a wonky thing to say but is actually very useful, even for the average person to consider what data may be getting out there about you, to really take the resources that are available online to look at your data profile. There are some companies that allow that. There are some that give you sort of your advertising profile.

Those resources are helpful but I think really the onus is on especially the government to lead the way by having the highest standard of privacy and security and then to create legal incentives for companies to protect and safeguard user data.

Ms. BONAMICI. Thank you so much, and my time has expired. I yield back.

Thank you, Madam Chair.

Chairwoman COMSTOCK. Okay. And now I recognize Mr. Palmer for five minutes.

Mr. PALMER. Thank you, Madam Chairman.

Following on that line of questioning, in the Anthem hack, the hackers got access to medical IDs and that is a little bit more problematic than just finding out what drugs people buy and whether or not they exercise, that sort of thing. Would it not create some issues in regard to violation of the HIPAA laws if a company bought that data and was able to specifically target advertising to people, for instance, who are diabetic or have certain other conditions? Let me address that Mr. Wright.

Mr. WRIGHT. I remember the initial creation of HIPAA and stuff and I know a lot of that dealt with the encryption. I am not an expert on HIPAA so I don't even want to pretend that I can answer that completely.

Mr. PALMER. Well, let me simplify it.

Mr. WRIGHT. Yes.

Mr. PALMER. It is against the law to disclose individual health—patient information.

Mr. WRIGHT. Correct.

Mr. PALMER. The doctor can't do it without your permission.

Mr. WRIGHT. Correct.

Mr. PALMER. He can't share it with anyone, and that medical ID could potentially get people access to that, that they would then sell that information. And it seems to me that if this is going on, there ought to be some legal recourse that either the government takes or the individuals take against companies who buy the data. It needs to go both ways, not just going after the hacker but going after the people who are buying the information. It is almost like buying fenced goods.

Mr. WRIGHT. Um-hum.

Ms. DE MOOY. Sir, I think one thing that would help would be some transparency into the system, which there is very little of it right now. Second, I would just say that HIPAA didn't apply in this case. The HealthCare.gov website was not a covered entity, which is—HIPAA is, you know, a really complicated law. I struggle to understand it. But I know that it did not fall under the categories of covered entities.

Mr. PALMER. Okay. And in that regard, when people are basically being forced into a system, does it not make sense that the government gives them an opportunity to opt out of providing certain data or even allowing their data to be shared?

Mr. WRIGHT. I think—and it should be very clear because you are on a government system. I mean it is about transparency because that information you are talking about, collection, can also be used to target a consumer from an individual standpoint of access to their medical records, their financial records. We know that these phishing attacks have been successfully done by the Chinese, by the Russians, by other folks targeting specific people. Unit 6139A specifically targeted people by a collection of a lot of information. The more information you can get it, it becomes—to a behavioral standpoint, I used to instruct behavioral analysis like out at the NSA. I will tell you this, that if I can get inside your mind and I can make you believe it is a legitimate email because I have enough detail and I can convince you, now I can compromise your identity.

That is the scary part about medical identity because now that the payment system will be coming online, the ability to commit fraud with somebody's medical identity, as the Chair pointed out, 10 times greater than straight identity theft, the value of that information.

Mr. PALMER. All right. In a report from last August—or August of last year, which I guess would be last August, HHS Inspector General found that the value of the 60 contracts that were issued to develop and operate HealthCare.gov totaled \$1.7 billion. At the end of last year Accenture was awarded a five-year contract to fix HealthCare.gov that totaled \$563 million. Altogether now we have spent at least \$2.3 billion on this failed website. How much do you estimate that it is going to cost to implement your suggestions to secure it?

Mr. WRIGHT. My original testimony back in November there is a rule of thumb that says if it costs \$1 to fix it before it is launched, it costs \$10 to fix it after it is launched. In an observation—

Mr. PALMER. I think it is going to be a little bit more than 10, though, so what—

Mr. WRIGHT. Well, I mean it is—what I am saying is that if a problem—

Mr. PALMER. It is a tenfold issue?

Mr. WRIGHT. It is a tenfold issue. So if it costs you \$1 million before launch you could have fixed it, it will cost you \$10 million after launch. And, you know, my dad was a World War II vet. They fought and completed World War II, built numerous ships, numerous—thousands, hundreds of thousands of planes and tanks with far less—in far less time, and my concern is this will keep going because they are not addressing the fundamental issues.

Mr. PALMER. I would like, if you don't mind, for you to get back to the Committee and give us a number. And in regard to your last point there, I used to work in engineering and we had a saying that there is never time to do it right but there is always time to do it over. Apparently, that is the case here.

Thank you, Madam Chairman.

Chairwoman COMSTOCK. Thank you.

And I yield to Mr. Tonko for five minutes.

Mr. TONKO. Thank you, Madam Chair.

The traffic to the federal government health insurance website was up 58 percent compared to the same time last week in a week-to-week measurement. That was some 275,000 individuals that signed up, making it the busiest enrollment period of the past two months, and the comparisons from last year to this year are “as an experience, pretty dramatic.” What is your reaction to that?

Ms. DE MOOY. My reaction is that the government should immediately implement some of these recommendations to make sure that no, as I said, American should have to choose between their data sharing and their health.

Mr. TONKO. Does it indicate any sort of comfort zone with the website?

Ms. DE MOOY. I think that is difficult to say. I think there is a deadline looming and so the government has tried to get as many people who need this service to make sure that it is in front of them and available to them. But the fact that they have reduced data sharing is good; they just need to do more.

Mr. TONKO. Um-hum. And it seems like over the past 10, 20 years the expectations of privacy have diminished dramatically. Do you think that that is true and what can we do to ensure that private personal data stay private?

Ms. DE MOOY. I don't think that is true. It is something that I hear quite a bit and I usually hear from people who have curtains and people who like to wear pants, for example, sort of not clever way but people care about privacy. It is a part of autonomy. It is at the heart of it. And when you take that autonomy away, in this example, where the government didn't ask or get permission, then you are removing a fundamental right that we have.

I think there are steps that—especially in the case of HealthCare.gov—that can be taken to ensure more privacy, to ensure autonomy and freedom, and so that when people go, they have the option of whether they want to share this kind of data. Certainly in the health context it is more sensitive.

I think companies have options. I think privacy is in itself an innovation. To speak to your point about making sure that we don't

limit innovation, you know, the internet, I remember a time when the internet was not something that people used to buy things from. It was literally too scary to do that but privacy became an innovation that allowed that to happen.

Mr. TONKO. Um-hum.

Ms. DE MOOY. And I think in this atmosphere of data sharing, rampant data sharing, that needs to happen once again.

Mr. TONKO. Ms. De Mooy, one of your recommendations that would address the wider problems beyond HealthCare.gov was to strengthen legal incentives for companies to better safeguard data. Can you speak more directly to this and what it would look like and why it is necessary?

Ms. DE MOOY. Sir, I think that is something I could get to you in writing. In our written testimony that sort of lays out some of our recommendations. And CDT has done quite a bit of work on policy in that and I think I would do it a disservice to sum it up now. But I can say that in the President's comprehensive Consumer Privacy Bill of Rights, what that did was create a framework for legislation around the fair information practice principles, which have guided privacy and security for decades and are sort of renowned as something that is flexible and nimble enough to address new technologies. I think that would be a start for there to be sort of a baseline consumer privacy legislation, something that we have been sorely lacking in the United States.

Mr. TONKO. And are there steps that you believe can be taken by private industry or commercial companies, internet providers to help limit the amount of personal data these enterprises collect?

Ms. DE MOOY. Absolutely. I think data minimization is a term that we use to describe when a company has a purpose for collecting a data point and that it stops collecting after that purpose has been fulfilled. It is a kind of simple concept but one that is lost, especially in the rampant data collection online. So implementing a real understanding of why you need a piece of data and not just collecting every single piece that you can get would drastically reduce the risks to people in terms of security and privacy.

Mr. TONKO. Um-hum. Is there a point where that could become unrealistic?

Ms. DE MOOY. Data minimization?

Mr. TONKO. Um-hum.

Ms. DE MOOY. To my understanding, no. I think data systems are designed from the beginning, and when they use privacy principles such as data minimization, it is very possible. You know, there is really no system that I know of the needs every single thing about you in order to function. Usually we use services and apps for a specific purpose. And so I think that is absolutely doable.

Mr. TONKO. Okay. Thank you very much, and with that, I yield back, Madam Chair.

Chairwoman COMSTOCK. Thank you.

And thank you to our witnesses.

I think we are supposed to have some votes sometime in the next few minutes here, so I think we will be able to close out now. But I really want to thank you and appreciate your expertise.

And while, you know, we might have in the normal order—certainly we ask the government to give us answers to the letters we sent, but I think your expertise and the information you provided I think will help illuminate that hearing, and so I hope any ideas you might have for us and questions to ask, that you will feel free to come forward because I think what you have demonstrated through your discussion and the expertise the you have is that we don't have to, nor should we have to make the choice between privacy and being able to use our modern technology.

I mean we have always been able to match technology with technology if we approach it with the right principles. That is sort of the new way we have to work on things in the 21st century. So I think the very specific things that you pointed out here and certainly doing this on the front end is much less costly. So I think as we set up practices I think it has been helpful for you to—the information you have given us and I look forward to our next testimony in light of the information you have given us.

And I do invite you to provide us with any additional information that you think might be helpful as we hear from the government, as we learn more going along. It would be helpful for us for the record.

And the record for this hearing will remain open two weeks for additional comments and written questions from Members. And the witnesses are excused and this hearing is adjourned. Thank you.

[Whereupon, at 4:04 p.m., the Subcommittees were adjourned.]

Appendix I

ANSWERS TO POST-HEARING QUESTIONS

ANSWERS TO POST-HEARING QUESTIONS

Responses by Ms. Michelle De Mooy

**Questions submitted by Rep. Barbara Comstock, Chairwoman,
Subcommittee on Research and Technology and Rep. Barry Loudermilk,
Chairman, Subcommittee on Oversight**

1) Effective tomorrow, should HealthCare.gov officials inform each and every individual with an account about the website's use of third-party tools, the specific information being collected, and elicit their specific permission to continue doing so?

Answer: All individuals should be informed about how and why their personal information is collected and shared, including users who visit HealthCare.gov. Ideally, HealthCare.gov would limit third-party data sharing to what is strictly necessary to operate the site; as I mentioned in my testimony, site analytics can be conducted internally on first-party data. At a minimum, the site should provide a clear description of how data is being collected and used by the website and by any third parties, and users should be given a choice about whether or not this is acceptable, with alternative access to comparable information and services if they choose to opt out.

This can be accomplished by directing users to an easy-to-read privacy policy that provides detail about their data collection, by sharing practices via notice to users who register at the site, in advance of any data collection or sharing, or a combination of these. In addition, the government should be constrained about the sharing of personal data, should be highly transparent, and should consider doing analytics or retargeting of any kind in-house in order to minimize privacy and security risks.

2) News stories have explained that there is no evidence that personal information from HealthCare.gov has been misused. However, how would federal officials know whether these data mining companies are selling, sharing, or otherwise misusing Americans' personal information? If a company does in fact engage in such practices, what recourse would consumers have?

Answer: Once information leaves a website server, it may not be possible for an entity to know how user information is shared or used. Contractual agreements can often provide insight into this but, in the case of HealthCare.gov, we don't know what these contracts said, if they even existed, or what auditing mechanisms may have been in place to limit data sharing or use.

Consumers have little to no recourse when it comes to stemming the bulk collection, sharing, and use of their personal information. Though they may benefit from adjusting settings on browsers, such as using Google Chrome's Incognito function or other browser add-ons that allows them to clear cookies or block third-party content or JavaScript, companies have found ways around some of these tools by using other tracking technologies. Ultimately, Congress can best protect consumer information by strengthening legal incentives for companies to better safeguard data and by enacting comprehensive data privacy

legislation that gives users more insight and control over how their information is collected and used.¹

3) In January, the White House issued a press release announcing, "President Obama will build on the steps he has taken to protect American companies, consumers, and infrastructure from cyber threats, while safeguarding privacy and civil liberties." Does this announcement comport with what you know of HealthCare.gov, particularly when it comes to privacy and security concerns?

Answer: It is clear that the privacy and security missteps that occurred on HealthCare.gov were avoidable. In addition to following guidance on third party sharing scenarios offered by the Office of Management and Budget (OMB), there are workable alternatives to third party sharing, such as performing analytics using only first party data collected on HealthCare.gov via software that does not send personal user information to the software maker. Another option would be creating sharing buttons that direct users to social media without sending user information to these sites.

A careful implementation of tried and true privacy principles, such as those offered by the Fair Information Practice Principles (FIPPs), could have mitigated or prevented the problems with HealthCare.gov. Specifically, the site should have used only individual data needed for functionality, restricted data sharing with third parties unless absolutely necessary, and adhered to rules that allow for user opt-outs or opt-ins and provide access to information without data sharing. The government should practice what it preaches by following the practical and privacy-protective guidance offered by OMB and should rewrite HealthCare.gov's privacy policy to make it responsive to these recommendations.

3) In a March 11, 2015 letter to the Committee, the Centers for Medicare and Medicaid Services explained that:

"We use third-party tools to better serve our consumers. Through the third-party tools, we work with private sector companies to provide insight into improving site performance and, during Open Enrollment, our outreach efforts to eligible consumers. As is common for consumer-facing websites, we use third-party tools and analyze HealthCare.gov's technical performance and to measure the effectiveness and cost-benefit of our outreach efforts."

Do other federal agencies utilize third-party tools for the purposes described above? Is so, how does their number of tools used compare to the number of tools used by HealthCare.gov?

¹ CDT's Analysis of the Consumer Privacy Bill of Rights, <https://cdt.org/insight/analysis-of-the-consumer-privacy-bill-of-rights-act/>

Answer: Some government websites utilize limited third-party tools for analytics or social sharing purposes. However, the number of third parties that were actively collecting personal information from visitors to HealthCare.gov without their knowledge or consent, went well and beyond what most government websites do. Catchpoint Systems found that user health information was being shared with 50 or more third party entities on HealthCare.gov, without user knowledge or permission. In comparison, Ghostery recently found many third parties receiving user information on 16 state insurance exchange sites, including personal health information². If CMS was using these tools for retargeting potential customers off the Healthcare.gov site that, too, would go beyond normal practice of government websites, and would probably exceed ordinary consumer expectations.

Government agencies have an obligation to uphold a high standard of privacy and security for visitors and users of their websites and services. Any third-party web application or analytics service installed on federal websites, such as those on HealthCare.gov, should insure that: 1) at a minimum, a PIA has been conducted and is easily available to visitors via the healthcare.gov privacy policy page; and, 2) limit the sharing of personal information to only what is strictly necessary to operate the site. The number of third-party content providers loading code into the browser of visitors to HealthCare.gov posed serious security issues, as well. Not only have researchers pointed to third-party content as one of the primary ways for websites to be infected with malware,³ compromising the integrity of third party content providers can accomplish a wide range of attacks, from simply changing the content of the page to capturing user information and credentials like passwords.⁴ Vendors without a direct relationship (and accountability) to the user are often the weakest link in the privacy and security chain.

² Kaye, Kate. *HealthCare.gov and State Sites Still Crawling with Ad Trackers*. AdAge, February 5, 2015. <http://adage.com/article/privacy-and-regulation/healthcare-gov-state-sites-crawling-ad-trackers/296982/>

Responses by Mr. Morgan Wright

HOUSE COMMITTEE ON SCIENCE, SPACE AND TECHNOLOGY
SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
SUBCOMMITTEE ON OVERSIGHT

"Can Americans Trust the Privacy and Security of their Information on HealthCare.gov?"

Responses of Mr. Morgan Wright, Principal, Morgan Wright, LLC

Questions submitted by Rep. Barbara Comstock, Chairwoman, Subcommittee on Research and Technology and Rep. Barry Loudermilk, Chairman, Subcommittee on Oversight

- 1) ANSWER: Yes. Compared to other government sites, HealthCare.gov obtains some of the most specific and personally identifiable information (PII) on consumers. The recent discovery of the excessive use of numerous tools to collect information – which resulted in the unencrypted transmission of key pieces of PII – does not engender the type of trust needed between consumers and the government.

Many companies who conduct business over the internet from time to time will change their privacy policies or terms and conditions for use of their website. When this happens, we have all seen the notices that say to effect "Continued use of this site constitutes your agreement..." or "By clicking 'Accept', this constitutes your agreement..." Consumers are given an option NOT to use a site. At a minimum, consumers should be given the option to 'opt out' of third-party tools that track specific and individual actions on their part.

- 2) ANSWER: In my opinion, the most critical is the finding that *"CMS did not conduct complete security testing."* You cannot manage what you cannot measure. The fact that a complete end-to-end security test has not been performed in an each of my earlier testimony before Congress on November 18, 2013.

The impact of failing to follow guidance can easily be demonstrated by the events leading up to my most recent testimony when it was discovered that PII was being transmitted unencrypted from the form that consumers were filling out as a preliminary step to obtaining coverage. This one flagrant oversight of a basic security control was discovered not by CMS, but by outside third parties and the news media. Simply following the guidance of NIST and OMB would have allowed CMS to put proper controls and reviews in place *before* putting into production key public-facing components of HealthCare.gov.

The real impact is the wasted time and taxpayer funds to respond to a security flaw discovered by the media and third parties, the hearings that resulted from this and the ongoing and persistent narrative of the lack of oversight and awareness of the most basic functions of HealthCare.gov. If you can't discover a 'rookie' mistake, how can you give the American people confidence that you can thwart and discover attacks and attempts by the real 'pros'?

- 3) ANSWER: There is no way to know without auditing the information collected by the data mining and measurement companies. To say there is 'no evidence' is to actually say "As far as we know...". The real question is how does CMS know? The fact is they don't. The only way to establish the ground truth is to have an aggressive and active audit and accountability function built into any agreement with third parties who provide tools to HealthCare.gov.

This was clearly not done. Simply relying on the unsworn word of third parties is insufficient when dealing with the PII of American taxpayers. Due to the lack of transparency on the collection of data and the lack of notification about it, this leaves little recourse for consumers to know their information has been improperly used. To think that a consumer could unravel the labyrinth of third-party connections by current and previously used third-party tools would make finding a needle in a haystack a trivial exercise.

- 4) ANSWER: This is a classic example of "Do as I say, not as I do". In my November 18, 2013 testimony before Congress I remarked:

"This is completely unacceptable from an industry perspective, and is in extreme contravention of security best practices. Only in the government could such a gaping hole be allowed to exist without fear of consequence. This shows a lack of understanding for the consequences to consumers and the protection of their PII. It also creates massive opportunity for fraud, scams, deceptive trade practices, identity theft and more. Much of this is playing out right now."

This one key passage from my testimony was also quoted by Sharyl Attkisson in her New York Times bestseller *Stonewalled*. Over one year later, with the amount of money spent on the site exceeding \$800M according to information provided during my testimony, little has changed.

- 5) ANSWER: I conducted a review of many sites prior to my testimony, including IRS.gov and WhiteHouse.gov. Almost every federal website I reviewed (30+) use some form of measurement – which is perfectly acceptable. However, when the news reports were released that showed HealthCare.gov was using over 50 third-party tools, the highest number of third-party tools used by federal websites I reviewed was 5. The IRS used 3. Arguably, the IRS holds PII considered being some of the most sensitive taxpayer and consumer information held by any government agency.

As a taxpayer and consumer, I do not object to third party tools being used to improve the performance and experience of a federal website. In fact, a major objection to using some sites is that they are anything but user-friendly and responsive. However, this is not about a private company collecting private data in exchange for something of perceived value in return. It is about a government agency with immense power collecting my PII without proper security controls and notifications in place. I have a choice with which website I go buy a computer from. I have no choice with health care.

Appendix II

ADDITIONAL MATERIAL FOR THE RECORD

PREPARED STATEMENT SUBMITTED BY SUBCOMMITTEE ON
RESEARCH AND TECHNOLOGY MEMBER ELIZABETH ESTY

Thank you to the Committee for holding this hearing on privacy and security concerns on HealthCare.Gov, and thank you to our witnesses for your time. Since so much of our personal business—from paying our credit cards to applying for mortgages to choosing health insurance—is now conducted online, it is all the more important that we maintain a strong cyber infrastructure to protect our security and personal privacy.

In Connecticut, we established our own health insurance marketplace, Access Health CT, for residents to shop for and secure health insurance. Over half a million Connecticut residents have already enrolled in health insurance plans through Access Health CT, and in 2014 our state's uninsured rate was cut in half. I am encouraged by the level of success we have achieved in Connecticut, and I look forward to working with my fellow Committee Members to ensure that Americans across the country have access to affordable healthcare without compromising their privacy and personal information.

LETTERS SUBMITTED BY SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY
CHAIRWOMAN BARBARA COMSTOCK

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

January 29, 2015

Hon. Shaun Donovan
Director
Office of Management and Budget
725 17th Street NW
Washington, DC 20503

Dear Mr. Donovan,

According to an *Associated Press* (AP) story published last week,¹ as many as 50 data mining companies were provided direct access to monitor information entered on the HealthCare.gov website. It appears this access was provided with permission and even encouragement from the federal government. Every American who has visited the Obamacare website may have been monitored by numerous companies without their consent or knowledge. This revelation raises serious questions about both personal privacy and cybersecurity on the HealthCare.gov website.

The AP reported that when a person applies for coverage through HealthCare.gov, approximately 50 data mining companies immediately become aware of the individual's online presence. Data mining companies can then search for sensitive personal information that applicants are required to enter. This can include a social security number, annual salary, employment, place of residence, immigration status, military service, criminal history, financial information, age, whether one is pregnant, whether one smokes and more.

Once a data mining company seizes this treasure trove of sensitive personal information, it is able to combine this data with other information collected by tapping into commercial websites and databases such as phone calls, texts, social media posts, frequently visited websites, and credit card purchases. These detailed electronic dossiers on millions of Americans could then be sold to other businesses, U.S. government agencies, foreign governments and even criminal enterprises that are willing to pay large sums of money for the information.

Data mining companies gather and sell personal information without our knowledge or consent. Indeed, one of the branches of the commercial cybersecurity industry focuses on the prevention of data mining. It is astonishing that the Obama administration has allowed scores of these companies to have embedded connections on the HealthCare.gov website.

¹ Ricardo Alonso-Zaldivar and Jack Gillum, "New Privacy Concerns Over Government's Health Care Website," AP News, January 20, 2015, available at: http://apnews.myway.com/article/20150120/us-health_overhaul-privacy-8b7c5d925b.html.

Mr. Donovan
January 29, 2015
Page Two

A spokesman for the Centers for Medicare and Medicaid Services (CMS) confirmed to AP that outside vendors were allowed on HealthCare.gov in order to provide feedback about website quality and user convenience. According to the spokesman, outside vendors “are prohibited from using information from these tools on HealthCare.gov for their companies’ purposes.”² Nevertheless, it isn’t clear how, or if, CMS is able to monitor what data mining companies are doing on HealthCare.gov.

Outside cybersecurity experts who commented for the AP story expressed surprise and concern that so many companies are permitted at HealthCare.gov, since website quality control assessments could be handled by just one or two outside firms. Experts pointed out that outside vendors are often the weak link for serious cybersecurity breaches – like the one that affected Target and millions of its customers. In the case of HealthCare.gov, a cybersecurity breach could threaten all of the federal agencies (e.g., the Internal Revenue Service) as well as the millions of Americans who visit the website.

The Federal Information Security Management Act of 2002 (FISMA) requires all federal agencies to develop and implement programs that secure their information and information systems. Under FISMA, each agency must conduct annual reviews of its information security program, and report the results to the Office of Management and Budget (OMB). OMB, in turn, has FISMA oversight responsibilities and must submit an annual report to Congress.

The National Institute of Standards and Technology (NIST), over which this Committee has jurisdiction, “develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and in managing cost-effective programs to protect their information and information systems.”³ Each agency’s information control system must be reviewed, certified and accredited under NIST publication SP 800-37, “Guide for the Security Certification and Accreditation of Federal Information Systems.”⁴ Security accreditation is required under OMB Circular A-130, Appendix III. Accredited systems must be monitored continuously, including ongoing assessment of security controls. By accrediting an agency’s information system, the responsible agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs.

Under FISMA, the Director of the OMB is required to oversee the information security policies and practices of federal agencies, which include “assessing the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information and information systems.”⁵ Given the Committee’s concerns over the privacy of individuals and cybersecurity ramifications of the presence of data mining companies on HealthCare.gov, I would appreciate answers to the following questions by February 6, 2015:

- 1) Before the AP news story, was OMB aware of the presence of data mining companies on HealthCare.gov?
- 2) Were you consulted about the decision to allow this? If not, who was consulted and who authorized this?

² Ibid.

³ NIST, Information Technology Laboratory, Computer Security Division, Computer Security Resource Center, FISMA Compliance, available at: <http://csrc.nist.gov/groups/SMA/fisma/compliance.html>.

⁴ NIST Special Publication 800-37, “Guide for the Security Certification and Accreditation of Federal Information Systems,” May 2004, available at: <https://www.fisimcenter.com/SP800-37-final.pdf>.

⁵ Public Law 107-347, available at: <http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>

Mr. Donovan
January 29, 2015
Page Three

- 3) What is the justification for authorizing embedded connections on HealthCare.gov for several dozen data mining companies, and should they be allowed continued access to Americans' information on HealthCare.gov?
- 4) How did CMS assess the risk from potential unauthorized use or disclosure of the personal details required on HealthCare.gov as a result of providing data mining companies access to HealthCare.gov?
- 5) What levels of information security are in place to protect the information on HealthCare.gov from unauthorized access, use or disclosure that were deemed appropriate by CMS, and are FISMA-compliant?

The Committee is posing questions similar to those above to CMS, the Office of Science and Technology Policy and the U.S. Department of Health and Human Services. If your staff has any questions, please contact Cliff Shannon, Staff Director of the Research and Technology Subcommittee, at Cliff.Shannon@mail.house.gov or (202) 226-9783.

Sincerely,



Lamar Smith
Chairman

cc: Eddie Bernice Johnson
Ranking Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371

www.science.house.gov

January 28, 2015

Hon. Sylvia M. Burwell
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Ms. Burwell,

According to an *Associated Press* (AP) story published last week,¹ as many as 50 data mining companies were provided direct access to monitor information entered on the HealthCare.gov website. It appears this access was provided with permission and even encouragement from the federal government. Every American who has visited the Obamacare website may have been monitored by numerous companies without their consent or knowledge. This revelation raises serious questions about both personal privacy and cybersecurity on the HealthCare.gov website.

The AP reported that when a person applies for coverage through HealthCare.gov, approximately 50 data mining companies immediately become aware of the individual's online presence. Data mining companies can then search for sensitive personal information that applicants are required to enter. This can include a social security number, annual salary, employment, place of residence, immigration status, military service, criminal history, financial information, age, whether one is pregnant, whether one smokes and more.

Once a data mining company seizes this treasure trove of sensitive personal information, it is able to combine this data with other information collected by tapping into commercial websites and databases such as phone calls, texts, social media posts, frequently visited websites, and credit card purchases. These detailed electronic dossiers on millions of Americans could then be sold to other businesses, U.S. government agencies, foreign governments and even criminal enterprises that are willing to pay large sums of money for the information.

Data mining companies gather and sell personal information without our knowledge or consent. Indeed, one of the branches of the commercial cybersecurity industry focuses on the prevention of data mining. It is astonishing that the Obama administration has allowed scores of these companies to take up permanent residence on the HealthCare.gov website.

A spokesman for the Centers for Medicare and Medicaid Services (CMS) confirmed to AP that outside vendors were allowed on HealthCare.gov in order to provide feedback about website quality and

¹ Ricardo Alonso-Zaldivar and Jack Gillum, "New Privacy Concerns Over Government's Health Care Website," AP News, January 20, 2015, available at: http://apnews.myway.com/article/20150120/us-health_overhaul-privacy-8b7c5d925b.html.

Ms. Burwell
January 28, 2015
Page two

user convenience. According to the spokesman, outside vendors "are prohibited from using information from these tools on HealthCare.gov for their companies' purposes."² Nevertheless, it isn't clear how, or if, CMS is able to monitor what data mining companies are doing on HealthCare.gov.

Outside cybersecurity experts who commented for the AP story expressed surprise and concern that so many companies are permitted at HealthCare.gov, since website quality control assessments could be handled by just one or two outside firms. Experts pointed out that outside vendors are often the weak link for serious cybersecurity breaches -- like the one that affected Target and millions of its customers. In the case of HealthCare.gov, a cybersecurity breach could threaten all of the federal agencies (e.g., the Internal Revenue Service) as well as the millions of Americans who visit the website.

The Federal Information Security Management Act of 2002 (FISMA) requires all federal agencies to develop and implement programs that secure their information and information systems. Under FISMA, each agency must conduct annual reviews of its information security program, and report the results to the Office of Management and Budget (OMB). OMB, in turn, has FISMA oversight responsibilities and must submit an annual report to Congress.

The National Institute of Standards and Technology (NIST), over which this Committee has jurisdiction, "develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and in managing cost-effective programs to protect their information and information systems."³ Each agency's information control system must be reviewed, certified and accredited under NIST publication SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems."⁴ Security accreditation is required under OMB Circular A-130, Appendix III. Accredited systems must be monitored continuously, including ongoing assessment of security controls. By accrediting an agency's information system, the responsible agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs.

Given the Committee's concerns over the privacy of individuals and cybersecurity ramifications of the presence of data mining companies on HealthCare.gov, I would appreciate answers to the following questions by February 6, 2015:

- 1) Before the AP news story, were you aware of the presence of data mining companies on HealthCare.gov?
- 2) Were you consulted about the decision to allow this? If not, who was consulted and who authorized this?
- 3) What is the justification for allowing several dozen data mining companies to inhabit HealthCare.gov and should they be allowed to continue occupying the website?

² Ibid.

³ NIST, Information Technology Laboratory, Computer Security Division, Computer Security Resource Center, FISMA Compliance, available at: <http://csrc.nist.gov/groups/SMA/fisma/compliance.html>.

⁴ NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," May 2004, available at: <https://www.fismacenter.com/SP800-37-final.pdf>.

Ms. Burwell
January 28, 2015
Page three

- 4) Are you aware of any CMS capability to monitor adequately the activities of the outside firms that are embedded in HealthCare.gov? Are you concerned that some of these companies may be gathering sensitive personal information from the millions of Americans who have applied for health insurance coverage on HealthCare.gov?
- 5) In your view, is CMS' decision to allow dozens of outside data mining companies on HealthCare.gov consistent with the Federal Information Security Management Act?
- 6) If CMS is not FISMA compliant for HealthCare.gov, what steps will be taken to achieve compliance and how soon?
- 7) How many of these private data mining companies have or have had access to the information on HealthCare.gov? In response to this question, please provide a list of all data mining companies on HealthCare.gov, including their specific role and reason for their presence on the website, and authorizations they were given by the government regarding the extent and types of data they could monitor and/or collect on HealthCare.gov, and what they were, or are, permitted to do with that information.
- 8) Further, please furnish all official communications with the data mining companies that have had access to HealthCare.gov, including with your office, the Centers for Medicare and Medicaid Services and the Office of Science and Technology Policy (OSTP).

The Committee is posing questions similar to those above to OSTP and CMS. In light of the serious issues of personal privacy and government information security raised by the recent news reports, the Committee may ask you to appear on relatively short notice and testify.

If your staff has any questions, please contact Cliff Shannon, Staff Director of the Research and Technology Subcommittee, at Cliff.Shannon@mail.house.gov or (202) 226-9783.

Sincerely,



Lamar Smith
Chairman

cc: Eddie Bernice Johnson
Ranking Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371
www.science.house.gov

January 28, 2015

Ms. Megan Smith
Chief Technology Officer
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue NW
Washington, DC 20504

Dear Ms. Smith,

According to an *Associated Press* (AP) story published last week,¹ as many as 50 data mining companies were provided direct access to monitor information entered on the HealthCare.gov website. It appears this access was provided with permission and even encouragement from the federal government. Every American who has visited the Obamacare website may have been monitored by numerous companies without their consent or knowledge. This revelation raises serious questions about both personal privacy and cybersecurity on the HealthCare.gov website.

The AP reported that when a person applies for coverage through HealthCare.gov, approximately 50 data mining companies immediately become aware of the individual's online presence. Data mining companies can then search for sensitive personal information that applicants are required to enter. This can include a social security number, annual salary, employment, place of residence, immigration status, military service, criminal history, financial information, age, whether one is pregnant, whether one smokes and more.

Once a data mining company seizes this treasure trove of sensitive personal information, it is able to combine this data with other information collected by tapping into commercial websites and databases such as phone calls, texts, social media posts, frequently visited websites, and credit card purchases. These detailed electronic dossiers on millions of Americans could then be sold to other businesses, U.S. government agencies, foreign governments and even criminal enterprises that are willing to pay large sums of money for the information.

Data mining companies gather and sell personal information without our knowledge or consent. Indeed, one of the branches of the commercial cybersecurity industry focuses on the prevention of data mining. It is astonishing that the Obama administration has allowed scores of these companies to take up permanent residence on the HealthCare.gov website.

¹ Ricardo Alonso-Zaldívar and Jack Gillum, "New Privacy Concerns Over Government's Health Care Website," AP News, January 20, 2015, available at: http://apnews.myway.com/article/20150120/us--health_overhaul-privacy-8b7c5d925b.html.

Ms. Smith
January 28, 2015
Page two

A spokesman for the Centers for Medicare and Medicaid Services (CMS) confirmed to AP that outside vendors were allowed on HealthCare.gov in order to provide feedback about website quality and user convenience. According to the spokesman, outside vendors "are prohibited from using information from these tools on HealthCare.gov for their companies' purposes."² Nevertheless, it isn't clear how, or if, CMS is able to monitor what data mining companies are doing on HealthCare.gov.

Outside cybersecurity experts who commented for the AP story expressed surprise and concern that so many companies are permitted at HealthCare.gov, since website quality control assessments could be handled by just one or two outside firms. Experts pointed out that outside vendors are often the weak link for serious cybersecurity breaches -- like the one that affected Target and millions of its customers. In the case of HealthCare.gov, a cybersecurity breach could threaten all of the federal agencies (e.g., the Internal Revenue Service) as well as the millions of Americans who visit the website.

The Federal Information Security Management Act of 2002 (FISMA) requires all federal agencies to develop and implement programs that secure their information and information systems. Under FISMA, each agency must conduct annual reviews of its information security program, and report the results to the Office of Management and Budget (OMB). OMB, in turn, has FISMA oversight responsibilities and must submit an annual report to Congress.

The National Institute of Standards and Technology (NIST), over which this Committee has jurisdiction, "develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and in managing cost-effective programs to protect their information and information systems."³ Each agency's information control system must be reviewed, certified and accredited under NIST publication SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems."⁴ Security accreditation is required under OMB Circular A-130, Appendix III. Accredited systems must be monitored continuously, including ongoing assessment of security controls. By accrediting an agency's information system, the responsible agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs.

Given the Committee's concerns over the privacy of individuals and cybersecurity ramifications of the presence of data mining companies on HealthCare.gov, I would appreciate answers to the following questions by February 6, 2015:

- 1) Before the AP news story, were you aware of the presence of data mining companies on HealthCare.gov?
- 2) Were you consulted about the decision to allow this? If not, who was consulted and who authorized this?
- 3) What is the justification for allowing several dozen data mining companies to inhabit HealthCare.gov and should they be allowed to continue occupying the website?

² Ibid.

³ NIST, Information Technology Laboratory, Computer Security Division, Computer Security Resource Center, FISMA Compliance, available at: <http://csrc.nist.gov/groups/SMA/fisma/compliance.html>.

⁴ NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," May 2004, available at: <https://www.fismacenter.com/SP800-37-final.pdf>.

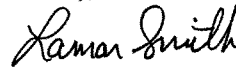
Ms. Smith
January 28, 2015
Page three

- 4) Are you aware of any CMS capability to monitor adequately the activities of the outside firms that are embedded in HealthCare.gov? Are you concerned that some of these companies may be gathering sensitive personal information from the millions of Americans who have applied for health insurance coverage on HealthCare.gov?
- 5) In your view, is CMS' decision to allow dozens of outside data mining companies on HealthCare.gov consistent with the Federal Information Security Management Act?
- 6) If CMS is not FISMA compliant for HealthCare.gov, what steps will be taken to achieve compliance and how soon?
- 7) How many of these private data mining companies have or have had access to the information on HealthCare.gov? In response to this question, please provide a list of all data mining companies on HealthCare.gov, including their specific role and reason for their presence on the website, and authorizations they were given by the government regarding the extent and types of data they could monitor and/or collect on HealthCare.gov, and what they were, or are, permitted to do with that information.
- 8) Further, please furnish all official communications with the data mining companies that have had access to HealthCare.gov, including with your office, the U.S. Department of Health and Human Services (HHS), and the Centers for Medicare and Medicaid Services.

The Committee is posing questions similar to those above to HHS and CMS. In light of the serious issues of personal privacy and government information security raised by the recent news reports, the Committee may ask you to appear on relatively short notice and testify.

If your staff has any questions, please contact Cliff Shannon, Staff Director of the Research and Technology Subcommittee, at Cliff.Shannon@mail.house.gov or (202) 226-9783.

Sincerely,


Lamar Smith
Chairman

cc: Eddie Bernice Johnson
Ranking Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371

www.science.house.gov

January 28, 2015

Hon. Marilyn Tavenner
Administrator
Centers for Medicare and Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244

Dear Ms. Tavenner,

According to an *Associated Press* (AP) story published last week,¹ as many as 50 data mining companies were provided direct access to monitor information entered on the HealthCare.gov website. It appears this access was provided with permission and even encouragement from the federal government. Every American who has visited the Obamacare website may have been monitored by numerous companies without their consent or knowledge. This revelation raises serious questions about both personal privacy and cybersecurity on the HealthCare.gov website.

The AP reported that when a person applies for coverage through HealthCare.gov, approximately 50 data mining companies immediately become aware of the individual's online presence. Data mining companies can then search for sensitive personal information that applicants are required to enter. This can include a social security number, annual salary, employment, place of residence, immigration status, military service, criminal history, financial information, age, whether one is pregnant, whether one smokes and more.

Once a data mining company seizes this treasure trove of sensitive personal information, it is able to combine this data with other information collected by tapping into commercial websites and databases such as phone calls, texts, social media posts, frequently visited websites, and credit card purchases. These detailed electronic dossiers on millions of Americans could then be sold to other businesses, U.S. government agencies, foreign governments and even criminal enterprises that are willing to pay large sums of money for the information.

Data mining companies gather and sell personal information without our knowledge or consent. Indeed, one of the branches of the commercial cybersecurity industry focuses on the prevention of data mining. It is astonishing that the Obama administration has allowed scores of these companies to take up permanent residence on the HealthCare.gov website.

A spokesman for the Centers for Medicare and Medicaid Services (CMS) confirmed to AP that outside vendors were allowed on HealthCare.gov in order to provide feedback about website quality and

¹ Ricardo Alonso-Zaldivar and Jack Gillum, "New Privacy Concerns Over Government's Health Care Website," AP News, January 20, 2015, available at: http://apnews.myway.com/article/20150120/us-health_overhaul-privacy-8b7c5d925b.html.

Ms. Tavenner
January 28, 2015
Page two

user convenience. According to the spokesman, outside vendors “are prohibited from using information from these tools on HealthCare.gov for their companies’ purposes.”² Nevertheless, it isn’t clear how, or if, CMS is able to monitor what data mining companies are doing on HealthCare.gov.

Outside cybersecurity experts who commented for the AP story expressed surprise and concern that so many companies are permitted at HealthCare.gov, since website quality control assessments could be handled by just one or two outside firms. Experts pointed out that outside vendors are often the weak link for serious cybersecurity breaches — like the one that affected Target and millions of its customers. In the case of HealthCare.gov, a cybersecurity breach could threaten all of the federal agencies (e.g., the Internal Revenue Service) as well as the millions of Americans who visit the website.

The Federal Information Security Management Act of 2002 (FISMA) requires all federal agencies to develop and implement programs that secure their information and information systems. Under FISMA, each agency must conduct annual reviews of its information security program, and report the results to the Office of Management and Budget (OMB). OMB, in turn, has FISMA oversight responsibilities and must submit an annual report to Congress.

The National Institute of Standards and Technology (NIST), over which this Committee has jurisdiction, “develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and in managing cost-effective programs to protect their information and information systems.”³ Each agency’s information control system must be reviewed, certified and accredited under NIST publication SP 800-37, “Guide for the Security Certification and Accreditation of Federal Information Systems.”⁴ Security accreditation is required under OMB Circular A-130, Appendix III. Accredited systems must be monitored continuously, including ongoing assessment of security controls. By accrediting an agency’s information system, the responsible agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs.

Given the Committee’s concerns over the privacy of individuals and cybersecurity ramifications of the presence of data mining companies on HealthCare.gov, I would appreciate answers to the following questions by February 6, 2015:

- 1) Before the AP news story, were you aware of the presence of data mining companies on HealthCare.gov?
- 2) Were you consulted about the decision to allow this? If not, who was consulted and who authorized this?
- 3) What is the justification for allowing several dozen data mining companies to inhabit HealthCare.gov and should they be allowed to continue occupying the website?

² Ibid.

³ NIST, Information Technology Laboratory, Computer Security Division, Computer Security Resource Center, FISMA Compliance, available at: <http://csrc.nist.gov/groups/SMA/fisma/compliance.html>.

⁴ NIST Special Publication 800-37, “Guide for the Security Certification and Accreditation of Federal Information Systems,” May 2004, available at: <https://www.fismacenter.com/SP800-37-final.pdf>.

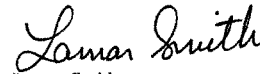
Ms. Tavenner
January 28, 2015
Page three

- 4) Are you aware of any CMS capability to monitor adequately the activities of the outside firms that are embedded in HealthCare.gov? Are you concerned that some of these companies may be gathering sensitive personal information from the millions of Americans who have applied for health insurance coverage on HealthCare.gov?
- 5) In your view, is CMS' decision to allow dozens of outside data mining companies on HealthCare.gov consistent with the Federal Information Security Management Act?
- 6) If CMS is not FISMA compliant for HealthCare.gov, what steps will be taken to achieve compliance and how soon?
- 7) How many of these private data mining companies have or have had access to the information on HealthCare.gov? In response to this question, please provide a list of all data mining companies on HealthCare.gov, including their specific role and reason for their presence on the website, and authorizations they were given by the government regarding the extent and types of data they could monitor and/or collect on HealthCare.gov, and what they were, or are, permitted to do with that information.
- 8) Further, please furnish all official communications with the data mining companies that have had access to HealthCare.gov, including with your office, the U.S. Department of Health and Human Services (HHS) and the Office of Science and Technology Policy (OSTP).

The Committee is posing questions similar to those above to OSTP and HHS. In light of the serious issues of personal privacy and government information security raised by the recent news reports, the Committee may ask you to appear on relatively short notice and testify.

If your staff has any questions, please contact Cliff Shannon, Staff Director of the Research and Technology Subcommittee, at Cliff.Shannon@mail.house.gov or (202) 226-9783.

Sincerely,


Lamar Smith
Chairman

cc: Eddie Bernice Johnson
Ranking Member

LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congress of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6301

(202) 225-6371

www.science.house.gov

January 29, 2015

Dr. Charles H. Romine
Director
Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, MS 8900
Gaithersburg, MD 20899

Dear Dr. Romine,

According to an *Associated Press* (AP) story published last week,¹ as many as 50 data mining companies were provided embedded connections to the HealthCare.gov website that enabled them to access personal information entered by individuals who applied for health insurance coverage. Every American who visited the Obamacare website, therefore, has been monitored by these companies without their consent or knowledge. This raises serious questions about both personal privacy protections and cybersecurity vulnerability on the HealthCare.gov website.

Data mining companies gather and sell personal information without our knowledge or consent. Indeed, one of the branches of the commercial cybersecurity industry focuses on the prevention of data mining. It is astonishing to me and other members of our committee that the Obama Administration has allowed scores of these companies to take up permanent residence on the HealthCare.gov website and harvest sensitive financial and health care information about millions of Americans. We are also concerned that a cybersecurity breach through a third party at HealthCare.gov could threaten not just the mass theft of millions of individual records but the security of computer systems at other federal agencies (e.g., the Internal Revenue Service).

A spokesman for the Centers for Medicare and Medicaid Services (CMS) confirmed to AP that outside vendors were allowed on HealthCare.gov in order to provide feedback about website quality and user convenience. According to the spokesman, outside vendors "are prohibited from using information from these tools on HealthCare.gov for their companies' purposes."² Nevertheless, it isn't clear how, or if, CMS is able to monitor what data mining companies are doing on HealthCare.gov.

The Committee solicits your views on these two issues. As a starting point, would you please comment on these questions?

¹ Ricardo Alonso-Zaldivar and Jack Gillum, "New Privacy Concerns Over Government's Health Care Website," AP News, January 20, 2015, available at: http://apnews.myway.com/article/20150120/us--health_overhaul-privacy-8b7c5d925b.html.

² Ibid.

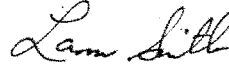
Dr. Romine
January 29, 2015
Page Two

- Does the embedded connectivity of 50 data mining companies at HealthCare.gov comport with the privacy provisions of the NIST Framework? As you pointed out in responding to a question posed at the recent Research and Technology Subcommittee hearing on cybersecurity, the Framework's privacy protection planks are "pretty strong." Nevertheless, the Framework may not consider the possibility of a federal government website furnishing personal information about millions of Americans to dozens of private companies. If not, perhaps the Framework's privacy provisions should be updated?
- Does HealthCare.gov's connections to so many third parties constitute a potentially significant vulnerability? Cyber attacks launched through third party systems have been employed on both public and private targets. As Ms. McGuire from Symantec noted during the same Subcommittee hearing, opening up HealthCare.gov to so many embedded third parties created "additional vulnerabilities." In your view, is the assertion of FISMA compliance affected or undermined by the large number of third party connections at HealthCare.gov?

The Committee is also posing questions to other involved agencies, including the officials at the Office of Science and Technology Policy, the Department of Health and Human Services, the Centers for Medicare and Medicaid Services, and the Office of Management and Budget. Because concerns about cybersecurity implications are immediate, I would appreciate it if you could provide a response to the above questions on or before February 6, 2015.


If your staff has any questions, please contact Cliff Shannon, Staff Director of the Research and Technology Subcommittee, at Cliff.Shannon@mail.house.gov or (202) 226-9783.

Sincerely,


Lamar Smith
Chairman

cc: Eddie Bernice Johnson
Ranking Member

Experts warn 2015 could be 'Year of the Healthcare Hack'

 REUTERS

By Caroline Hummer and Jim Finkle | Reuters -- 22 hours ago

(Reuters) - Security experts are warning healthcare and insurance companies that 2015 will be the "Year of the Healthcare Hack," as cybercriminals are increasingly attracted to troves of personal information held by U.S. insurers and hospitals that command high prices on the underground market.

Anthem Inc, the No. 2 U.S. health insurer, last week disclosed a massive breach of its database containing nearly 80 million records, prompting investigations by state and federal authorities. That hack followed a breach last year at hospital operator Community Health Systems, which compromised some 4.5 million records.

"People feel that this will be the year of medical industry breaches," said Dave Kennedy, chief executive of TrustedSEC LLC.

In the past decade, cybercriminals focused their efforts on attacking banks and retailers to steal financial data including online banking credentials and payment card numbers. But as those companies boost security, using stolen credit card numbers has become more difficult.

Their prices on criminal exchanges have also dropped, prompting hackers to turn to the less-secure medical sector, just as the amount of digital healthcare data is growing dramatically, Kennedy said.

Stolen healthcare data can be used to fraudulently obtain medical services and prescriptions as well as to commit identity theft and other financial crimes, according to security experts. Criminals can also use stolen data to build more convincing profiles of users, boosting the success of scams.

"All of these factors are making healthcare information more attractive to criminals," said Rob Sadowski, marketing director at RSA, the security division of EMC Corp.

Monetizing stolen data

RSA Executive Chairman Art Coviello recently wrote in a letter to customers that he expected well-organized cybercriminals to turn their attention to stealing personal information from healthcare providers.

"A name, address, social and a medical identity ... That's incredibly easy to monetize fairly quickly," said Bob Gregg, CEO of ID Experts, which sells identity protection software and services. Identities can sell for \$20 apiece, or more, he said.

Insurers, medical equipment makers and other companies say they have been preparing for breaches after seeing the waves of attacks on other industries.

Cigna Corp has looked to financial and defense companies for best practices, including hiring hackers to break into its systems, said Chief Executive David Cordani. Attempts to break into corporate systems to probe for information are a constant, he said in an interview.

St Jude Medical Inc CEO Daniel Starks said the company increased investment in cybersecurity significantly over the last few years, to protect both patient data and the medical devices it manufactures.

"You may see from time to time law enforcement briefings on nation-based (intellectual property) issues, espionage," he said. "Those are things that we take very seriously and have been briefed on and that we work to guard against."

The FBI is investigating the Anthem breach alongside security experts from FireEye Inc.

The insurers UnitedHealth Group Inc and Aetna Inc have warned investors about the risks of cyber crime in their annual reports since 2011.

UnitedHealth has said the costs to eliminate or address the threats could be significant and that remediation may not be successful, resulting in lost customers.

In response to the Anthem attack, UnitedHealth spokesman Tyler Mason said in an emailed statement: "We are in close contact with our peers in ... the industry cybersecurity organization, and are monitoring our systems and the situation closely."

Aetna has cited the automated attempts to gain access to public-facing networks, denial of service attacks that seek to disrupt websites, attempted virus infections, phishing and efforts to infect websites with malicious content.

Aetna spokeswoman Cynthia Michener said in a statement: "We closely follow the technical details of every breach that's reported to look for opportunities to continually improve our own IT security program and the health sector's information protection practices broadly."

(Additional reporting by Bill Berkrot in New York; editing by Michele Gershberg and G Crosse)

the WHITE HOUSE PRESIDENT BARACK OBAMA

BRIEFING ROOM ISSUES THE ADMINISTRATION PARTICIPATE 1600 PENN

Home • Briefing Room • Presidential Actions • Executive Orders

The White House
Office of the Press Secretary

For Immediate Release

May 09, 2013

**Executive Order -- Making Open and Machine Readable the
New Default for Government Information**

EXECUTIVE ORDER

MAKING OPEN AND MACHINE READABLE THE NEW DEFAULT
FOR GOVERNMENT INFORMATION

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. General Principles. Openness in government strengthens our democracy, promotes the delivery of efficient and effective services to the public, and contributes to economic growth. As one vital benefit of open government, making information resources easy to find, accessible, and usable can fuel entrepreneurship, innovation, and scientific discovery that improves Americans' lives and contributes significantly to job creation.

Decades ago, the U.S. Government made both weather data and the Global Positioning System freely available. Since that time, American entrepreneurs and innovators have utilized these resources to create navigation systems, weather newscasts and warning systems, location-based applications, precision farming tools, and much more, improving Americans' lives in countless ways and leading to economic growth and job creation. In recent years, thousands of Government data resources across fields such as health and medicine, education, energy, public safety, global development, and finance have been posted in machine-readable form for free public use on Data.gov. Entrepreneurs and innovators have continued to develop a vast range of useful new products and businesses using these public information resources, creating good jobs in the process.

To promote continued job growth, Government efficiency, and the social good that can be gained from opening Government data to the public, the default state of new and modernized Government information resources shall be open and machine readable. Government information shall be managed as an asset throughout its life cycle to promote interoperability and openness, and, wherever possible and legally permissible, to ensure that data are released to the public in ways that make the data easy to find, accessible, and usable. In making this the new

default state, executive departments and agencies (agencies) shall ensure that they safeguard individual privacy, confidentiality, and national security.

Sec. 2. Open Data Policy. (a) The Director of the Office of Management and Budget (OMB), in consultation with the Chief Information Officer (CIO), Chief Technology Officer (CTO), and Administrator of the Office of Information and Regulatory Affairs (OIRA), shall issue an Open Data Policy to advance the management of Government information as an asset, consistent with my memorandum of January 21, 2009 (Transparency and Open Government), OMB Memorandum M-10-06 (Open Government Directive), OMB and National Archives and Records Administration Memorandum M-12-18 (Managing Government Records Directive), the Office of Science and Technology Policy Memorandum of February 22, 2013 (Increasing Access to the Results of Federally Funded Scientific Research), and the CIO's strategy entitled "Digital Government: Building a 21st Century Platform to Better Serve the American People." The Open Data Policy shall be updated as needed.

(b) Agencies shall implement the requirements of the Open Data Policy and shall adhere to the deadlines for specific actions specified therein. When implementing the Open Data Policy, agencies shall incorporate a full analysis of privacy, confidentiality, and security risks into each stage of the information lifecycle to identify information that should not be released. These review processes should be overseen by the senior agency official for privacy. It is vital that agencies not release information if doing so would violate any law or policy, or jeopardize privacy, confidentiality, or national security.

Sec. 3. Implementation of the Open Data Policy. To facilitate effective Government-wide implementation of the Open Data Policy, I direct the following:

(a) Within 30 days of the issuance of the Open Data Policy, the CIO and CTO shall publish an open online repository of tools and best practices to assist agencies in integrating the Open Data Policy into their operations in furtherance of their missions. The CIO and CTO shall regularly update this online repository as needed to ensure it remains a resource to facilitate the adoption of open data practices.

(b) Within 90 days of the issuance of the Open Data Policy, the Administrator for Federal Procurement Policy, Controller of the Office of Federal Financial Management, CIO, and Administrator of OIRA shall work with the Chief Acquisition Officers Council, Chief Financial Officers Council, Chief Information Officers Council, and Federal Records Council to identify and initiate implementation of measures to support the integration of the Open Data Policy requirements into Federal acquisition and grant-making processes. Such efforts may include developing sample requirements language, grant and contract language, and workforce tools for agency acquisition, grant, and information management and technology professionals.

(c) Within 90 days of the date of this order, the Chief Performance Officer (CPO) shall work with the President's Management Council to establish a Cross-Agency Priority (CAP) Goal to track implementation of the Open Data Policy. The CPO shall work with agencies to set incremental performance goals, ensuring they have metrics and milestones in place to monitor advancement toward the CAP Goal. Progress on these goals shall be analyzed and reviewed by agency leadership, pursuant to the GPRA Modernization Act of 2010 (Public Law 111-352).

(d) Within 180 days of the date of this order, agencies shall report progress on the implementation of the CAP Goal to the CPO. Thereafter, agencies shall report progress quarterly, and as appropriate.

Sec. 4. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department, agency, or the head thereof; or

Executive Order -- Making Open and Machine Readable the New Def... <http://www.whitehouse.gov/the-press-office/2013/05/09/executive-ord...>

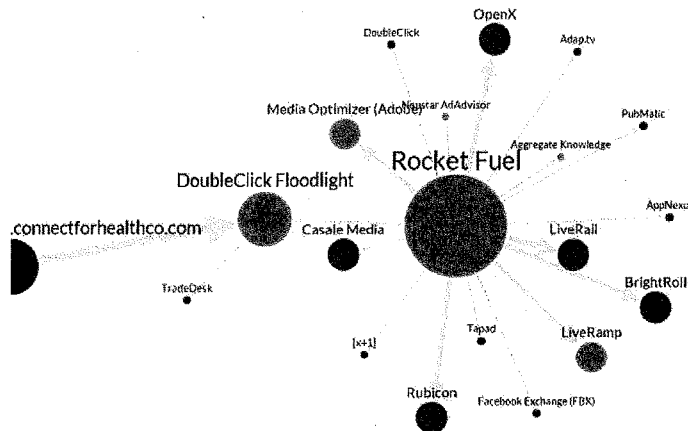
- (ii) the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.
- (b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.
- (c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.
- (d) Nothing in this order shall compel or authorize the disclosure of privileged information, law enforcement information, national security information, personal information, or information the disclosure of which is prohibited by law.
- (e) Independent agencies are requested to adhere to this order.

BARACK OBAMA

AdvertisingAge

Healthcare.gov and State Sites Still Crawling With Ad Trackers Facebook's Ad Exchange and Several Others Spotted on State Healthcare Sites

Published: February 05, 2015



Trackers Spotted by Ghostery on ConnectForHealthCO.com on January 28, 2015

People visiting Healthcare.gov, Colorado's ConnectForHealthCO, California's CoveredCA or NYStateofHealth lately might get more than information on health insurance plans: they might get ads on Facebook or just about anywhere else they're traveling online, based on the fact that they visited the health sites.

In the wake of an Associated Press report revealing that the federal government's Healthcare.gov site was exposing personal user data, that site along with 16 state

healthcare sites still have lots of ad trackers installed from companies including Facebook, Twitter and Google's Doubleclick.

During the week of Jan. 24 through Jan. 29, the federal healthcare site had 25 tracking technologies embedded, according to Ghostery, which evaluates the amount of tracking technologies on sites and can show where that information flows in real-time. That period follows reports that the Centers for Medicare and Medicaid Services said it had enhanced site encryption and limited the amount of information flowing to third-party technologies used for site analytics and advertising.

Between Jan. 7 and 14, Healthcare.gov had far more tracking systems installed – 52 as observed by Ghostery. By January 30, though, ad trackers including Twitter Advertising, RocketFuel, and Advertising.com were still spotted on pages where people can submit personal information.

The White House referred Ad Age to a statement made by The Centers for Medicare and Medicaid Service on January 24: "One of the most cost-effective and best ways to reach the uninsured is through digital media and advertising," stated Kevin Counihan, director and marketplace CEO at CMS. "To do this well, we have contracts with companies that help us to connect interested consumers to HealthCare.gov and continuously measure and improve site performance and our outreach efforts." He went on to say the agency is evaluating additional actions to improve consumer privacy.

Justin Brookman, director of the Consumer Privacy Project at the Center for Democracy and Technology, called it "bad site design," noting, "Given that they collect such sensitive data, and given that they're government services where people might not have a choice about visiting, I feel like these sites should really only share data with third parties when absolutely necessary."

Several statewide sites established as a result of the Affordable Care Act are also flooded with outside commercial technologies that cookie site visitors and pass that data along to ad-tech partners. Ghostery data reveals that between the period of January 7-14 and January 24-29, the number of tracking technologies spotted on Colorado's ConnectForHealthCO.com actually rose from 25 to 32.

One tracker added to the Colorado site in that time is LiveRamp, a company owned by data-services giant Acxiom that connects online user data to information companies have about their consumers from offline sources – such as purchasing data or information from retail loyalty programs -- for online ad targeting and ad-campaign measurement. A LiveRamp tag seen on Healthcare.gov in early January was removed by Jan. 24, according to Ghostery.

California, a state whose Attorney General Kamala Harris has been outspoken on digital

privacy issues, had the LiveRamp technology installed on its healthcare site throughout the month of January, during which time the number of trackers it had embedded dropped from 30 to 23. In late January, tags from ad platforms including Doubleclick, BlueKai and Advertising.com appeared on the California site, according to Ghostery.

California, New York and Colorado did not respond to requests for comment for this story.

Ghostery tracked several pages on Healthcare.gov and the 16 state sites, including pages where people supply sensitive personal information. Rhode Island's and Oregon's healthcare sites had eight and seven trackers in the last week of January, respectively. The remaining state sites had five or fewer trackers, some used for site measurement and analytics and some that pass information to advertising exchanges.

Yet one thing is clear: many of the technologies whose tags are embedded on these sites are not used for site operations or analytics purposes, but for advertising. That means at the most basic level, ad technologies tracking visitors to the federal and state health sites can help advertisers such as insurance brokers or other health or medical companies target ads to people who visited government healthcare sites, adding them to audience segments based on interest in health insurance or specific health and medical services.

For instance, both New York's and Colorado's health sites were spotted with Facebook Exchange tags in the last week of January. At the very least, that would enable the state sites themselves to send ads to people who have visited those sites, while they're on Facebook.

Simply expressing interest in health coverage and providing contact information to some state sites including CoverOregon, can result in a barrage of phone calls from health insurance brokers that receive those sales leads through the site.

"Each of these sites is clearly marketed and any sophisticated marketer is going to use a multichannel strategy," said Ghostery CEO Scott Meyer. "This is what you'd expect to see with a big digital marketing campaign."

My Way News - New privacy concerns over government's health care... http://apnews.myway.com/article/20150120/us--health_overhaul-priv..

My Way

page took 0.12 seconds • [home](#) | [my page](#) |

news | [home](#) | [top](#) | [world](#) | [intl](#) | [natl](#) | [op](#) | [pol](#) | [govt](#) | [business](#) | [tech](#) | [sci](#) | [entertain](#) | [sports](#) | [health](#) | [odd](#) | [sources](#) | [loc](#)
[AP](#) • [New York Times](#) • [MSNBC](#) • [USA TODAY](#) • [AP Hi Tech](#)

New privacy concerns over government's health care website

Jan 20, 4:56 AM (ET)

By RICARDO ALONSO-ZALDIVAR and JACK GILLUM

WASHINGTON (AP) — A little-known side to the government's health insurance website is prompting renewed concerns about privacy, just as the White House is calling for stronger cybersecurity protections for consumers.

It works like this: When you apply for coverage on HealthCare.gov, dozens of data companies may be able to tell that you are on the site. Some can even glean details such as your age, income, ZIP code, whether you smoke or if you are pregnant.

The data firms have embedded connections on the government site. Ever-evolving technology allows for individual Internet users to be tracked, building profiles that are a vital tool for advertisers.

Connections to multiple third-party tech firms were documented by technology experts who analyzed HealthCare.gov, and confirmed by The Associated Press. There is no evidence that personal information from HealthCare.gov has been misused, but the number of outside connections is raising questions.

"As I look at vendors on a website...they could be another potential point of failure," said corporate cybersecurity consultant Theresa Payton. "Vendor management can often be the weakest link in your privacy and security chain."

A former White House chief information officer under President George W. Bush, she said the large number of outside connections on HealthCare.gov seems like "overkill" and makes it "kind of an outlier" among government websites.

The privacy concerns come against the backdrop of President Barack Obama's new initiative to protect personal data online, a highlight of his State of the Union message scheduled for Tuesday night. The administration is getting the health care website ready for the final enrollment drive of 2015, aiming to have more than 9 million people signed up by Feb. 15 for subsidized private coverage.

Medicare spokesman Aaron Albright said outside vendors "are prohibited from using information from the tools on HealthCare.gov for their companies' purposes." The government uses them to measure the performance of HealthCare.gov so consumers get "a simpler, more streamlined and intuitive experience added."

The administration did not explain how it ensures that privacy and security policies are being followed.

Third-party outfits that track website performance are a standard part of e-commerce. HealthCare.gov's policy says in boldface that "no personally identifiable information is collected" by these web measurement tools.



(AP) This Nov. 12, 2014 file photo shows the HealthCare.gov website, which prompts people to register for 2015 coverage. [Full Image](#)

Google sponsored link

Register for RSAC 2015
 Over 350 sessions on info security Register now and \$400!
www.rsaconference.com/

Long Term Care Insurance
 Compare & Save with Free Quotes by the Best Provider in Your Area.
www.completelongtermcare.com

My Way News - New privacy concerns over government's health care... http://apnews.myway.com/article/20150120/us--health_overhaul-priv...

But in a recent visit to the site, AP found that certain personal details — including age, income, and whether you smoke — were being passed along likely without your knowledge to advertising and Web analytics firms.

Google said Monday it doesn't use that kind of data or allow its systems to target ads based on health or medical history information. "When we learn of possible violations of this policy, we investigate and take action," the company said in a statement.

Still, the outside connections surprised a tech expert who evaluated HealthCare.gov's performance for AP.

"Anything that is health-related is something very private," said Mehdi Daoudi, CEO of Catchpoint Systems. "Personally, I look at this, and I am on a government website, and I don't know what is going on between government and Facebook, and Google, and Twitter. Why is that there?"

Created under the president's health care law, HealthCare.gov is the online gateway to government-subsidized private insurance for people who lack coverage on the job.

Tracking consumers' Internet searches is a lucrative business, helping Google, Facebook and others tailor customers' interests. Because your computer and mobile devices can be assigned an individual signature, profiles of Internet users can be pieced together, generating lists that have commercial value.

Third-party sites embedded on HealthCare.gov can't see your name, birth date or Social Security number, but they may be able to correlate the fact that your computer accessed the government website with your other Internet activities.

Have you been researching a chronic illness like coronary artery blockage? Do you shop online for smoking cessation aids? Are you investigating genetic markers for a certain type of breast cancer? Are you seeking help for financial problems, or for an addiction?

Daoudi's company — Catchpoint Systems — came across some 50 third-party connections embedded on HealthCare.gov. They attracted attention because such connections can slow down websites. They work in the background, unseen to most consumers.

The AP was able to replicate the results. In one 10-minute visit to HealthCare.gov recently, dozens of websites were accessed behind the scenes. They included Google's data-analytics service, Twitter, Facebook and a number of online advertising providers.

Aldo Cortesi, a security consultant who reviewed the AP's findings, found a number of third-party trackers could log a user's actions in detail. Cortesi said there can be legitimate uses for such trackers, but said questions linger over the level of detailed information that could be sent to private parties.

"Third-party embedded websites are troubling because they can be used to track you and track your behavior when you're browsing the Web," said Cooper Quintin, a staff technologist with the Electronic Frontier Foundation, a civil liberties group.

"I think that this could erode ... confidentiality when dealing with medical data and medical information," Quintin, who also reviewed the AP's results.

HealthCare.gov is currently serving consumers in 37 states, while the remaining states operate their own insurance markets. The administration has set a nationwide goal of 9.1 million people signed up through insurance exchanges this year and paying their premiums.

Google sponsored links

HealthCare.gov Sends Personal Data to Dozens of Tracking Websites |... <https://www.eff.org/deeplinks/2015/01/healthcare.gov-sends-personal-...>



JANUARY 20, 2015 | BY COOPER QUINTIN

HealthCare.gov Sends Personal Data to Dozens of Tracking Websites

The [Associated Press](#) reports that healthcare.gov—the flagship site of the Affordable Care Act, where millions of Americans have signed up to receive health care—is quietly sending personal health information to a number of third party websites. The information being sent includes one's zip code, income level, smoking status, pregnancy status and more.

	event=16668199&=16668199&=fakeSrc=js&2219631051+222936070&8171652904-fakeSrc=171674651+none&171946872-g&172159083-direct&26904250-true...	GET	200	OK	166681991
	activitysrc=4037109;cat=20142003;ord=7917385912018;-oref=https://www.healthcare.gov/see-plans/85601/results/?county=04019&age=40&smoker=1&parent=&pregnant=1&mec=&zip=85601&state=AZ&income=35000&step=4?	GET	200	OK	4037109.fl
	Random=142146406378&cv=7&fv=142146406378&num=1&mt=1&guid=CH&u_b=9000u_y=16000u_shf=https://4037109.fl.doubleclick.net/activitysrc=4037109;type...	GET	302	Found	googleads.g
	ping=healthcare.gov&=see-plans/85601/results/?county=04019&age=40&smoker=1&parent=&pregnant=1&mec=&zip=85601&state=AZ&income=35000&step=4?	GET	200	OK	ping.chartbe

An example of personal health data being sent to third parties from healthcare.gov

EFF researchers have independently confirmed that healthcare.gov is sending personal health information to at least 14 third party domains, even if the user has enabled [Do Not Track](#). The information is sent via the referrer header, which contains the URL of the page requesting a third party resource. The referrer header is an essential part of the HTTP protocol, and is sent for every request that is made on the web. The referrer header lets the requested resource know what URL the request came from. This would for example let a website know who else was linking to their pages. In this case however the referrer URL contains personal health information.

In some cases the information is also sent embedded in the request string itself, like so:

```
https://4037109.fl.doubleclick.net/activityi;src=4037109;
type=20142003;cat=201420;ord=7917385912018;-oref=https://www.
healthcare.gov/see-plans/85601/results/?county=04019&age=40&
smoker=1&parent=&pregnant=1&mec=&zip=85601&state=AZ&
income=35000&step=4?
```

HealthCare.gov Sends Personal Data to Dozens of Tracking Websites |... <https://www.eff.org/deeplinks/2015/01/healthcare.gov-sends-personal>.

In the above example, a URL at doubleclick.net is requested by your browser. Appended to the end of this URL is your age, smoking status, pregnancy status, parental status, zip code, state and annual income. This URL is requested by your browser after you fill out the required information on healthcare.gov and click the button to view health insurance plans that you are eligible for.

The following is a table showing which third party domains EFF researchers confirmed were receiving the private health data.

Domain	PII in referrer	PII in request
Akamai.net	✓	
Chartbeat.net	✓	✓
Clicktale.net	✓	
DoubleClick.net	✓	✓
Google.com	✓	✓
Mathtag.com	✓	
Mixpanel.com	✓	
Nrd-data.net	✓	
Optimizely.com	✓	✓
Reson8.com	✓	
Rfihub.com	✓	
Twitter.com	✓	
Yahoo.com	✓	
Youtube.com	✓	



Sending such personal information raises significant privacy concerns. A company like Doubleclick, for example, could match up the personal data provided by healthcare.gov with an already extensive trove of information about what you read online and what your buying preferences are to create an extremely detailed profile of exactly who you are and what your interests are. It could do all this based on a tracking cookie that it sets which would be the same across any site you visit. Based on this data, Doubleclick could start showing you smoking ads or infer your risk of cancer based on where you live, how old you are and your status as a smoker.¹ Doubleclick might start to show you ads related to pregnancy, which could have embarrassing and potentially dangerous consequences such as when Target notified a woman's family that she was pregnant before she even told them.

It's especially troubling that the U.S. government is sending personal information to commercial companies on a website that's touted as the place for people to obtain health care coverage. Even more troubling is the potential for companies like Doubleclick, Google, Twitter, Yahoo, and others to associate this data with a person's actual identity. Google, thanks to real name policies, certainly has information uniquely identifying someone using Google services. If a real identity is linked to the information received from healthcare.gov it would be a massive violation of privacy for users of the site.

Third-party resources could also introduce additional security risks to the healthcare.gov

HealthCare.gov Sends Personal Data to Dozens of Tracking Websites |... [https://www.eff.org/deeplinks/2015/01/healthcare.gov-sends-personal...](https://www.eff.org/deeplinks/2015/01/healthcare.gov-sends-personal-...)

website, with each included third-party resource increasing the attack surface of the site. If an attacker were able to compromise just one of the third party resources included on healthcare.gov they could potentially compromise the accounts of every user of healthcare.gov. The attacker could then sell the Private Health Information or hold it for ransom.

For now, EFF recommends installing software that will block third party tracking, such as EFF's own Privacy Badger. Privacy badger will block the referrers and the connections to third party sites on healthcare.gov and protect your personal health information.

Health information is some of the most sensitive and personal information there is. People's private medical data should not be available to third party companies without consent from the user. This practice is negligent at best, and potentially devastating for consumers. At a minimum, healthcare.gov should disable third-party trackers for any user that requests an opt out using the DNT header. Arguably, healthcare.gov should meet good privacy standards for all its users.

President Obama will give his State of the Union speech tonight, in which he is expected to address cybersecurity issues. If President Obama is really concerned about cybersecurity, he may want to start in his own backyard, by securing healthcare.gov.



1. Update 2015-01-21: Google has told us that although Doubleclick does log and retain this data, the company doesn't use it for choosing which ads to display. This does not reduce our privacy and security concerns about the practices of healthcare.gov and its many embedded third parties.

[Do Not Track](#) [Medical Privacy](#) [The Law and Medical Privacy](#) [Online Behavioral Tracking](#)

MORE DEEPLINKS POSTS LIKE THIS

JUNE 2013

[How Dozens of Companies Know You're Reading About Those NSA Leaks](#)

SEPTEMBER 2009

[How Online Tracking Companies Know Most of What You Do Online \(and What Social Networks Are Doing to Help Them\)](#)

JANUARY 2015

[How Verizon and Turn Defeat Browser Privacy Protections](#)

FEBRUARY 2012

RECENT DEEPLINKS POSTS

FEB 10, 2015

[EFF Vows to Continue the Fight Against Mass Surveillance After Disappointing Ruling](#)

FEB 10, 2015

[Oakland Considers a Privacy Policy for its Domain Awareness \(Surveillance\) Center](#)

FEB 9, 2015

[An Exemption to the DMCA Would Let Game Fans Keep Abandoned Games Running](#)

HealthCare.gov Privacy Policy

Protecting your privacy is very important to us. We're telling you about HealthCare.gov's privacy policy so you know what information we collect, why we collect it, and what we do with it.

HealthCare.gov doesn't collect any personally identifiable information (PII) about you during your visit to our website unless you choose to provide it to us. We do, however, collect information from visitors who read, browse, and/or download information from our site. We do this so we can understand how the public uses the site and how to make it more helpful.

Healthcare.gov never collects information for commercial marketing or any purpose unrelated to our mission and goals.

Types of information we collect

When you browse through any website, certain information about your visit can be collected. We automatically collect and temporarily store the following types of information about your visit:

- Domain from which you access the Internet
- IP address (an IP or internet protocol address is a number that is automatically given to a computer connected to the Web)
- Operating system on your computer and information about the browser you used when visiting the site
- Date and time of your visit
- Pages you visited
- Address of the website that connected you to HealthCare.gov (such as google.com or bing.com)

We use this information to measure the number of visitors to our site and its various sections and to help make our site more useful to visitors.

How HealthCare.gov uses information it collects

HealthCare.gov uses a variety of Web measurement software tools. We use them to collect the information listed in the "Types of information collected" section above. The tools collect information automatically and continuously. **No personally identifiable information is collected by these tools.**

The HealthCare.gov staff analyzes and reports on the collected data from these tools. The reports are available only to HealthCare.gov managers, members of the HealthCare.gov communications and Web teams, and other designated staff who need this information to perform their duties.

HealthCare.gov also uses an online survey to collect opinions and feedback. This online survey appears on the bottom left of many pages on the site. You don't have to answer these questions. Please do not include any personally identifiable information (PII) in comments you make. We analyze and use this information to improve the site's operation and content. The reports are available only to HealthCare.gov managers, members of the communications and Web teams, and other designated staff who require this information to perform their duties.

HealthCare.gov keeps the data from our measurement tools as long as needed to support the mission of the website.

How HealthCare.gov uses cookies

The Office of Management and Budget Memo M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies, allows federal agencies to use session and persistent cookies.

When you visit any website, its server may generate a piece of text known as a "cookie" to place on your computer. The cookie allows the server to "remember" specific information about your visit while you are connected. The cookie makes it easier for you to use the dynamic features of Web pages. Cookies from

HealthCare.gov pages collect only information about your browser's visit to the site. They do not collect personal information about you.

There are two types of cookies, single session (temporary), and multi-session (persistent). Session cookies last only as long as your Web browser is open. Once you close your browser, the cookie disappears. Persistent cookies are stored on your computer for longer periods.

- **Session Cookies:** We use session cookies for technical purposes such as to allow better navigation through our site. These cookies let our server know that you are continuing a visit to our site. The OMB Memo 10-22 Guidance defines our use of session cookies as "Usage Tier 1—Single Session." The policy says, "This tier encompasses any use of single session web measurement and customization technologies."
- **Persistent Cookies:** We use persistent cookies to understand the differences between new and returning HealthCare.gov visitors. Persistent cookies remain on your computer between visits to our site until they expire. The OMB Memo 10-22 Guidance defines our use of persistent cookies as "Usage Tier 2—Multi-session without Personally Identifiable Information (PII)." The policy says, "This tier encompasses any use of multi-session Web measurement and customization technologies when no PII is collected."

How to opt out or disable cookies

If you do not wish to have session or persistent cookies placed on your computer, you can disable them using your Web browser. If you opt out of cookies, you will still have access to all information and resources at HealthCare.gov. Instructions for disabling or opting out of cookies in the most popular browsers are located at http://www.usa.gov/optout_instructions.shtml.

Please note that by opting out of cookies, you will disable cookies from all sources, not just from HealthCare.gov.

How we protect your personal information

You do not have to give us personal information to visit HealthCare.gov. However, if you choose to receive alerts or e-newsletters, we collect your email address to complete the subscription process.

If you choose to provide us with personally identifiable information through an email message, request for information, paper or electronic form, questionnaire, survey, etc., we will maintain the information you provide only as long as needed to respond to your question or to fulfill the stated purpose of the communication.

If in order to contact you we store your personal information in a record system designed to retrieve information about you by personal identifier (name, personal email address, home mailing address, personal or mobile phone number, etc.), we will safeguard the information you provide in accordance with the Privacy Act of 1974, as amended (5 U.S.C. Section 552a).

If HealthCare.gov operates a record system designed to retrieve information about you in order to accomplish its mission, a Privacy Act Notification Statement should be prominently and conspicuously displayed on the public-facing website or form which asks you to provide personally identifiable information. The notice must address the following five criteria:

1. HealthCare.gov legal authorization to collect information about you
2. Purpose of the information collection
3. Routine uses for disclosure of information outside of HealthCare.gov
4. Whether the request made of you is voluntary or mandatory under law
5. Effects of non-disclosure if you choose to not provide the requested information

For further information about HealthCare.gov privacy policy, please contact Privacy@cms.hhs.gov (<mailto:Privacy@cms.hhs.gov>).

Data safeguards and privacy

All uses of Web-based technologies comply with existing privacy and data

safeguarding policies and standards. Information Technology (IT) systems owned and operated by the Centers for Medicare & Medicaid Services (CMS) are assessed using Privacy Impact Assessments (PIAs) posted for public view on the Department of Health and Human Services (HHS) website (<http://www.hhs.gov/pia>). CMS conducts and publishes a PIA for each use of a third-party website and application (TPWA) as they may have a different functionality or practice. TPWA PIAs are posted for public view on the HHS website at <http://www.hhs.gov/pia>.

Groups of records that contain information about an individual and are designed to be retrieved by the individual's name or other personal identifier linked to the individual are covered by the Privacy Act of 1974, as amended (5 U.S.C. Section 552a). For these records, CMS Systems of Record Notices are published in the Federal Register and posted on the CMS Senior Official for Privacy Website.

When you visit CMS sites, please look for the Privacy Notice posted on the main pages. When Web measurement and customization technologies are used, the Privacy Policy/Notice must provide:

- Purpose of the web measurement and/or customization technology
- Usage tier, session type, and technology used
- Nature of the information collected
- Purpose and use of the information
- Whether and to whom the information will be disclosed
- Privacy safeguards applied to the information
- Data retention policy for the information
- Whether the technology is enabled by default or not and why
- How to opt out of the web measurement/customization technology
- Statement that opting out still permits users to access comparable information or services
- Identities of all third-party vendors involved in the measurement and

customization process

How long we keep data and how we access it

HealthCare.gov will keep data collected long enough to achieve the specified objective for which they were collected. The data generated from these activities falls under the National Archives and Records Administration (NARA) General Records Schedule (GRS) 20-item IC "Electronic Records," and will be handled according to the requirements of that schedule (<http://www.archives.gov/records-mgmt/grs/grs20.html>).

How HealthCare.gov uses third-party websites and applications

As a response to OMB Memo M-10-06, Open Government Directive, HealthCare.gov uses a variety of technologies and social media services to communicate and interact with citizens. These third-party website and application (TPWA) tools include popular social networking and media sites, open source software communities, and more. Examples include Facebook, Twitter, and YouTube.

TPWAs are not exclusively operated or controlled by HealthCare.gov. Users of TPWAs often share information with the general public, user community, and/or the third party operating the website. These actors may use this information in a variety of ways. TPWAs could cause PII to become available or accessible to HealthCare.gov and the public, regardless of whether the information is explicitly asked for or collected by us.

HealthCare.gov sometimes collects and uses your PII if you made it available through third-party websites. However, we do not share PII made available through third-party websites. Your activity on the third-party websites we use is governed by the security and privacy policies of those sites. You should review the third-party privacy policies before using the sites and ensure that you understand how your information may be used.

If you have an account with a third-party website and choose to "like," "friend,"

follow, or comment, certain PII associated with your account may be made available to HealthCare.gov based on the privacy policy of the third-party website and your privacy settings within that website. You should adjust privacy settings on your account to match your preferences.

We also collect **non**-personally identifiable information through the use of tracking pixels that appear on our pages. A tracking pixel is a transparent graphic image (usually 1 pixel x 1 pixel) that is placed on a web page and, in combination with a cookie, allows us to collect information regarding the use of the web page that contains the tracking pixel.

We use tracking pixels to tell when an advertisement we run on another website has been clicked on or otherwise interacted with. We use that information to judge which advertisements are more appealing to users. To opt out of these tracking pixels, please see the section above titled "How to opt out or disable cookies."

Links to other sites

HealthCare.gov links to other HHS sites, other government sites, and occasionally to private organizations. Once you leave HealthCare.gov, you are subject to the privacy policy for the sites you are visiting. HHS is not responsible for the contents of any off-site web page. A link to a page does not constitute an endorsement.

Additional Privacy information

- If you are an applicant on the individual Marketplace, read our [Individual Privacy Act statement \(/individual-privacy-act-statement\)](#).
- If you are an agent or broker, read our [Agent and Broker Privacy Act statement \(/agent-privacy-act-statement\)](#).
- Learn more about [how we use your individual Marketplace information \(/how-we-use-your-data\)](#).
- If you are an employer applying in the Small Business Health Options Program, read our [SHOP Employer Privacy Statement \(/shop-privacy-](#)

act-statement). You can also learn more about how we use your SHOP information ([/how-we-use-your-data-SHOP-employer](#)).

Can we improve this page?

A federal government website managed by the U.S.
Centers for Medicare & Medicaid Services, 7500
Security Boulevard, Baltimore, MD 21244

BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES



Interim Progress Report

February 2015

One year ago, President Obama spoke at the Department of Justice about changes in the technology we use for national security and signals intelligence purposes, and what those technological changes mean for privacy writ large. Recognizing that these technologies have implications beyond the national security arena, the President also called for a wide-ranging review of big data and privacy to explore how these technologies are changing our economy, our government, and our society, and to consider their implications for personal privacy. The goal of the review was to understand what is genuinely new and different about big data and to consider how best to encourage the potential of these technologies while minimizing risks to privacy, fair treatment, and other core American values.

Over the course of the 90-day inquiry, the big data and privacy working group—led by Counselor to the President John Podesta, Commerce Secretary Penny Pritzker, Energy Secretary Ernest Moniz, the President's science advisor Dr. John Holdren, and the President's economic advisor Jeff Zients—sought public input and engaged with academic researchers and privacy advocates, regulators and the technology industry, and advertisers and civil rights groups. The review was supported by a parallel effort by the President's Council of Advisors on Science and Technology (PCAST) to investigate the scientific and technological dimensions of big data and privacy.

The big data and privacy working group's report found that the declining cost of data collection, storage, and processing, coupled with new sources of data from sensors, cameras, and geospatial technologies, means that we live in a world where data collection is nearly

ubiquitous, where data retention can be functionally permanent, and where data analysis is increasingly conducted in speeds approaching real time. While there are promising technological means to better protect privacy in a big data world, the report's authors concluded these methods are far from perfect, and technology alone cannot protect privacy absent strong social norms and a responsive policy and legal framework. Finally, the report raised issues around other values potentially implicated by big data technology—particularly with regard to the potential for big data technologies to lead, purposely or inadvertently, to discriminatory outcomes on the basis of race, gender, socioeconomic status, or other categories.

But big data technologies continue to hold enormous promise, as the report identified—to streamline public services, to advance health care and education, and to combat fraud and complex crimes like human trafficking. A year after the President's request for this report, the Obama Administration has worked to advance a number of the concrete policy proposals offered in the report, both by launching new efforts and continuing to develop previously existing projects. The Administration continues to drive the national conversation, inside and outside of government, on how to maximize benefits while minimizing the risks and harms posed by a big data world.

Key Recommendations

The big data and privacy working group report identified six specific policy recommendations as deserving prompt action:

- **Advance the Consumer Privacy Bill of Rights** because consumers deserve clear, understandable, reasonable standards for how their personal information is used in the big data era.
- **Pass National Data Breach Legislation** that provides for a single national data breach standard, along the lines of the Administration's 2011 Cybersecurity legislative proposal.
- **Extend Privacy Protections to non-U.S. Persons** because privacy is a worldwide value, and should be reflected in how the federal government handles personally identifiable information from non-U.S. citizens.
- **Ensure Data Collected on Students in School is used for Educational Purposes** to protect students from having their data shared or used inappropriately.
- **Expand Technical Expertise to Stop Discrimination** so that the federal government's lead civil rights and consumer protection agencies can identify practices and outcomes facilitated by big data analytics that have a discriminatory impact on protected classes, and develop plans for investigating and resolving violations of law.
- **Amend the Electronic Communications Privacy Act** to ensure the standard of protection for online, digital content is consistent with that afforded in the physical world—including by removing archaic distinctions between email left unread or over a certain age.

The Administration is making significant progress on most of these recommendations:

- The Department of Commerce solicited public comment on the Consumer Privacy Bill of Rights in light of new technologies, including those identified in the big data and privacy report, and the Obama Administration will release draft legislation in early 2015.
- President Obama released revised national data breach legislation, the Personal Data Notification & Protection Act, on January 12, 2015.
- Attorney General Eric Holder announced in June 2014 that the Administration would seek legislation extending to EU citizens the same right to judicial redress for intentional or willful wrongful disclosure of personal data exchanged under the U.S.-EU Data Protection and Privacy Agreement for law enforcement purposes, or for refusal to grant access or to rectify any errors in that information, as U.S. citizens would have under the Privacy Act of 1974. The Office of Management and Budget is working with departments and agencies to extend other privacy protections to non-U.S. citizens.
- President Obama announced the Student Digital Privacy Act, a national effort to ensure K-12 student data is used only for educational purposes, on January 12, 2015, in conjunction with new private sector commitments to help enhance privacy for students as well as a landmark voluntary effort by over 100 companies committing not to abuse education data.
- Several efforts have been undertaken to further the federal government's understanding of big data and discrimination, including studying the potential implications of using predictive analytics in law enforcement at the Department of Justice and by studying price discrimination at the Council of Economic Advisers. The White House Domestic Policy Council is preparing a follow-on report for release in early 2015 focusing on the potential of big data both to lead to discriminatory outcomes in key policy areas and to be used to counteract discrimination.

Further progress on implementing the big data and privacy report's recommendations and related efforts is detailed in the following pages.

1. Preserving Privacy Values

The innovation driven by big data creates both tremendous opportunity and novel privacy challenges. The report explored privacy challenges across sectors, and suggested that we reexamine our conception of notice and consent, as well as the notion of use frameworks as a basis for managing privacy rights. The report suggested a number of specific steps forward in order to ensure that privacy protections evolve in a way that enables the social good that can result from big data, while protecting and empowering citizens.

Advance the Consumer Privacy Bill of Rights

The report called on the Department of Commerce to advance the 2012 Consumer Privacy Bill of Rights by seeking public comment on big data developments and how they impact the CPBR's policies and then devise draft legislative text. This month, the Administration plans to release draft legislation based on public comments received during that comment period.

Pass National Data Breach Legislation

The report called for the creation of a national data breach standard to benefit both consumers and businesses, in the face of a growing number of breaches and an inconsistent patchwork of state laws. In January 2015, President Obama announced the Personal Data Notification & Protection Act, a new legislative proposal to help bring peace of mind to all Americans, including the tens of millions whose personal and financial information has been compromised in a data breach. This proposal clarifies and strengthens the obligations companies have to notify customers when their personal information has been compromised, while providing companies with the certainty of a single, national standard—as well as criminalizing the illicit overseas trade in identities.

Bring Greater Transparency to the Data Services Industry

In May, the Federal Trade Commission released an in-depth report on the data broker industry, concluding that data brokers operate with a fundamental lack of transparency. The Commission recommended that Congress consider enacting legislation to make data broker practices more visible to consumers and to give consumers greater control over the personal information collected and shared by data brokers.

Lead International Conversations on Big Data

Data privacy has long been a component of the United States' bilateral and multilateral discussions. Well before the big data and privacy report, the Administration engaged in extensive consultation with data protection authorities, international civil society, and privacy experts from Europe and around the world.

Of particular note since the release of the report, high-ranking officials from the United States and Germany discussed the report's findings and bilateral cooperation on cyber issues as part of the third Cyber Bilateral Meeting in June 2014, including cybersecurity and critical infrastructure protection, cyber defense, combating cybercrime, Internet freedom, and Internet governance.

Extend Privacy Protections to non-U.S. Persons

The report recommended that the OMB work with agencies to apply the Privacy Act to non-U.S. persons where practicable, or establish alternative privacy policies for personal data held by the federal government that provide appropriate and meaningful protections regardless of nationality. OMB has been leading an interagency process to implement this recommendation.

In addition to these general protections, the United States is actively pursuing efforts to grant certain rights of judicial redress to EU citizens and citizens of other nations that effectively share terrorism and law enforcement information with the United States and provide appropriate privacy protections. In the 2014 U.S.-EU Ministerial Meeting on Justice and Home Affairs, Attorney General Eric Holder made clear the United States' commitment to pursue this effort, and the Administration is working closely with members of Congress on this important measure.

2. Responsible Educational Innovation in the Digital Age

"[D]ata collected on students in the classroom should only be used for educational purposes — to teach our children, not to market to our children. We want to prevent companies from selling student data to third parties for purposes other than education. We want to prevent any kind of profiling that puts certain students at a disadvantage as they go through school."

- President Barack Obama at the Federal Trade Commission, January 12, 2015

Big data has the potential to transform education for the better, creating unprecedented educational opportunities—for instance, by tailoring lessons to a student's learning style, by opening up courses through online platforms, and by making it easier for parents, teachers, and students to identify where an individual student may be struggling and offer targeted instruction. These new technologies hold the potential to vastly improve student performance and to provide researchers with valuable insights about how students learn, which could help improve low-tech educational interventions as well. Beyond educational technology, the mere operation of schools produces vast amounts of data—data that can improve efficiency as well as education. However, the federal government must play its part to ensure that student data is not shared or used inappropriately. The Administration has taken significant steps to safeguard student data in the classroom and beyond, as well as promoting and enabling innovation in learning.

Ensure Data Collected on Students in School is used for Educational Purposes

On January 12, 2015, the President proposed the Student Digital Privacy Act: a new legislative proposal designed to provide teachers and parents the confidence they need to enhance teaching and learning with the best technology—by ensuring that data collected in the educational context is used only for educational purposes. This bill, modeled on a landmark California statute, builds on the recommendations of the report, would prevent companies from selling student data to third parties for purposes unrelated to the educational mission and from engaging in targeted advertising to students based on data collected in school—while still permitting important research initiatives to improve student learning outcomes, and efforts by companies to continuously improve the effectiveness of their learning technology products.

The legislation will be accompanied by new tools from the Department of Education to empower educators around the country. The Department of Education and its Privacy Technical Assurance Center play a critical role in protecting American children from invasions of privacy in the classroom. Alongside the President's call for legislation, he unveiled executive actions that will enhance that office's abilities to help ensure educational data is used in ways appropriate and in accordance with the educational mission—including a model terms of service and providing teacher training assistance.

The largest educational technology vendors also committed to help lead the way in ensuring the protection of students—and, as of today, over 100 of them have signed on to a pledge to provide important protections against misuse of students' data.

Recognize Digital Literacy as an Important 21st Century Skill

Knowledge and efficient use of digital materials will become increasingly important as computer technologies begin to drive economic and educational empowerment. This recommendation was included in both the big data and privacy working group's recommendations and in the PCAST report. The Administration has advanced several initiatives that encourage digital literacy by connecting Americans to the latest technologies and strengthening the technical skills that can enable fluid use of the latest digital resources. These initiatives promote: (1) the literacy to help students be creators—not just consumers—with increased access to coding experiences, as the President illustrated by participating in the Hour of Code in fall 2014; (2) the literacy to be prepared to work in the STEM fields, through initiatives such as the President's Educate to Innovate campaign; (3) the literacy to use technology smartly, including empowering students to protect their privacy; and (4) literacy realized as access for all, including access to broadband at home and at school, an issue the President has tackled through the ConnectED Initiative. Connectivity is especially critical, as these initiatives must help bridge the digital divide and inequality of opportunity that often exists in educational contexts throughout the nation.

In the coming months, the White House will continue to work with stakeholders and other partners to develop new initiatives to make digital literacy opportunities more accessible and available for the American people.

3. Big Data and Discrimination

One of the most notable findings of the big data and privacy report was that alongside its potential benefits to be used to increase access to credit or improve educational outcomes, there also exists the potential for big data technology to be used to discriminate against individuals, whether intentionally or inadvertently, potentially enabling discriminating outcomes, reducing opportunities and choices available to them.

As part of the national discussion prompted by the big data study, the civil rights community, industry and federal agencies began to identify possible principles and frameworks to guide uses of data. Before the report was completed, a coalition of civil rights organizations announced a set of civil rights principles for the big data era, focused on stopping high-tech profiling, ensuring fairness in automated decisions, preserving constitutional principles, enhancing individual control

of personal information, and protecting people from inaccurate data. The civil rights community worked with technologists and academics to organize an October 2014 conference on big data and discrimination and hopes to make it an annual event, with continuing strong participation from the federal government.

The White House considers this topic a priority, and is continuing to explore the implications of big data in this arena, including considering how big data technology can be used to shore up civil rights. Among other investments, the Obama Administration's budget for Fiscal Year 16 includes \$17 million for data science pilots at the National Science Foundation that seek to study issues around data interoperability; data policy and governance; and data security, privacy, integrity, and trustworthiness. These pilots will directly inform other federal big data research projects and will assist in developing the technological and policy expertise needed to tackle difficult problems like the potential for big data to lead to discriminatory outcomes.

Pay Attention to the Potential for Big Data to Facilitate Discrimination

The White House Domestic Policy Council and the Office of Science and Technology Policy will issue a follow-up report further exploring the implications of big data technologies for discrimination and civil rights. Specifically, the new report will take a deeper dive into how big data interacts with issues like employment and access to credit—considering both how the use of big data technologies can perpetuate discrimination and prevent it. The White House has engaged with leading researchers and advocates to develop recommendations on actions that can be taken to use big data to broaden opportunity and to prevent discrimination.

Expand Technical Expertise to Stop Discrimination

One of the key recommendations of the big data and privacy report was that the federal government's lead civil rights and consumer protection agencies should expand their technical expertise to be able to identify practices and outcomes facilitated by big data analytics that may have a discriminatory impact on protected classes, and develop a plan for investigating and resolving potential violations of law.

In June, the Office of Science and Technology Policy and the Georgetown University McCourt School of Public Policy's Massive Data Institute cohosted a fourth big data convening focused on the work of federal agencies. The multi-stakeholder workshop focused on federal agencies' use of open data and big data, best practices for sharing data within and between agencies and other partners, and how to address potential privacy and civil liberties concerns that arise from the use of big data.

In September, the Federal Trade Commission hosted a workshop entitled "Big Data: A Tool for Inclusion or Exclusion?" in its Washington offices. The workshop explored the use of big data and its impact on American consumers, with an eye towards low income and underserved consumers. The workshop highlighted concerns about whether big data may be used to categorize consumers in ways that may affect them unfairly, or even unlawfully.

Deepen Understanding of Differential Pricing

The White House Council of Economic Advisors conducted a study of commercial applications of

big data. The CEA explored whether companies will use the information they harvest to more effectively charge different prices to different customers. The economic literature on value-based price discrimination suggests that this will often, though not always, be welfare-enhancing for both businesses and consumers. However, individualized pricing based on estimates of cost or riskiness can raise concerns about fairness, particularly when consumers are unaware of the data or methods that companies employ. The CEA report finds that many companies already use big data for targeted marketing, and some are experimenting with personalized pricing, though examples of personalized pricing remain fairly limited.

4. Law Enforcement and Security

Big data can be used to make our communities safer and strengthen our national security, but raises equally important questions for our personal privacy and civil liberties. The big data and privacy report encouraged our national security, homeland security, law enforcement, and intelligence communities to vigorously experiment with and employ lawful big data technology while adhering to full accountability, oversight, and relevant privacy requirements.

Review Law Enforcement's Use of Predictive Analytics

In light of the report, the Department of Justice recently conducted a review of the current use of predictive analytics in law enforcement. This review focused on the DOJ's own use of analytic tools, as well as on some of the programs the Department helps fund through research grants. DOJ also reviewed some of the newer technologies in use by state and local law enforcement agencies.

DOJ concluded that new data-driven technologies have the potential to bring significant benefits to our criminal justice system. Many of these technologies build on traditional techniques and are designed to help law enforcement agencies allocate scarce resources more efficiently to prevent crime. The Department also observed that the use of predictive analytics raises issues and potential challenges that are worthy of continued attention, so that predictive techniques continue to be driven by the core enforcement goals of protecting the public and ensuring fairness in our justice system.

Going forward, DOJ will work collaboratively with stakeholders and develop guidance for the use of predictive analytics by state and local law enforcement agencies. The Department will also continue to engage in ongoing conversations about the effectiveness and impact of new predictive techniques.

Foster Responsible Use and Privacy Best Practices with State and Local Law Enforcement Entities Receiving Federal Grants

The big data and privacy report recommended that that federal agencies with expertise in privacy and data practices provide technical assistance to state, local, and other federal law enforcement agencies seeking to deploy big data techniques. In November 2014, DOJ developed a supplemental guide to augment its privacy-related technical assistance library for state, local, and tribal law enforcement agencies, entitled *Resource Guide for Enhancing Community*

Relationships and Protecting Privacy and Constitutional Rights. This supplemental guide serves as a point of reference for state, local, and tribal law enforcement entities in fostering the development of responsible privacy practices. Additionally, DOJ continues to engage in outreach to state, local, and tribal law enforcement entities through participation in trainings and conferences on related issues.

Review Government Use of Commercial Databases

The report recommended that the federal government review uses of commercially available databases on U.S. citizens, focusing on use of services that employ big data techniques and ensuring that they incorporate appropriate oversight and protections for privacy and civil liberties. DOJ and the Office of the Director of National Intelligence, together with the Office of Management and Budget, are leading an effort to review the use of commercial databases by the federal government. In particular, they are examining the use of commercial databases by federal agencies in the context of public administration, law enforcement, and national security. The review process will include recommendations for how the government can use the databases while also protecting privacy and civil liberties.

Implement Best Practices for Controlled Use and Storage of Data at Agencies

Efforts are underway on several fronts to maximize privacy protections by improving agency use and storage of data, and to strengthen cybersecurity in general. For instance, the Department of Homeland Security is working across government and the private sector to identify and leverage the opportunities big data analytics presents to strengthen cybersecurity. This will include coordinating the development or changes of necessary policies to ensure that data is appropriately protected and secured.

The Office of Management and Budget is leading an effort to expand successful data management and security pilots across government and has connected practitioners and leaders from innovative and effective data management initiatives at several federal agencies to foster an exchange of success stories and lessons learned.

The National Security Council is asking the President's National Security Telecommunications Advisory Committee to undertake a private sector-led study with recommendations on using big data analytics to strengthen cybersecurity.

The Administration has also continued to address the challenges to information sharing. The Department of Justice and the Federal Trade Commission issued guidance that sharing of cyber threat information should not raise anti-trust concerns—thus addressing a long-standing concern from industry. The Department of Homeland Security is modernizing its Protected Critical Infrastructure Information program to enable its use for the protection of private sector information voluntarily submitted to the Department for the purposes of improving network defenses.

Advance Cybersecurity and Consumer Protection with 2015 Summit

On February 13, 2015, the White House will host a cybersecurity and consumer protection summit at Stanford University. The summit will bring together major stakeholders on cybersecurity and consumer financial protection issues from the public and private sectors to discuss a range of

topics, including creating improved cybersecurity practices and strengthening cyber threat information sharing. The summit will also serve as the next step in the President's BuySecure Initiative, will help advance national efforts the government has led on consumer financial protection and critical infrastructure cybersecurity, and will build on efforts to improve cybersecurity at a wide range of companies.

5. Data as a Public Resource

The report urged agencies across government to consider data as a national, public resource, and make it broadly available to the public wherever possible. This effort continues the Obama Administration's commitment to open data and open government from the first day of this Administration. To date, there are over 134,000 datasets available on Data.gov for public use. The Administration has made great strides towards bringing technologists into government through the creation of the United States Digital Service, 18F, and the Presidential Innovation Fellowship to ensure that the government continues to meet the needs of Americans who expect the high quality digital content, as well as make data open and usable to the public.

Continue Making Government Data Available to the Public

The Administration has launched a series of Open Data Initiatives that have unleashed large volumes of valuable data in areas such as health, energy, education, public safety, finance, and global development. For example, the Climate Data Initiative, launched in March 2014, leverages open climate data to fuel innovation and private sector entrepreneurship to advance climate change preparedness and community resilience through the development of data products, tools, and applications that are geared toward solving real-life challenges.

This Administration is committed to making open and machine-readable data the default for government information. Federal agencies have continued to increase the quantity and quality of open data over the past year. Each quarter, federal agencies add additional datasets to their Public Data Listings. Data.gov automatically updates its inventory by harvesting the Public Data Listings each day. Nearly every agency has data listed on Data.gov.

Adopting Open Data Best Practices

Many federal agencies have adopted new open data processes to better manage their data at an organizational level. For example, over the past year, NASA has continued to develop an agency-level NASA Information Architecture Management (NIAM) process to share and reuse data from across agency components. Through the NIAM process, NASA significantly improved its common metadata, contract language, and search capacity, and as a result, NASA increased its Enterprise Data Inventory from 25 datasets to more than 3,800 datasets between November 2013 and November 2014.

Increased customer engagement is helping to improve the federal open data policy. For example, agencies have learned that one of the most common complaints of data users is the use of PDF—rather than machine-readable—formats. OMB and OSTP are now working with agencies to reduce the number of PDFs and make machine-readability the standard for all government data.

Issues Needing Further Attention

Some efforts await Congressional or stakeholder action. For instance, efforts on Capitol Hill to amend the almost 30-year-old Electronic Communications Privacy Act have seen little progress since the report was issued. The report recommended that Congress amend ECPA to ensure the standard of protection for online, digital content is consistent with that afforded in the physical world—including by removing archaic distinctions between email left unread or over a certain age.

In 2012, the Administration expressed support for the multistakeholder development of a Do Not Track standard that could be used by consumers regardless of browser preference or operating system. This was a novel multi-stakeholder effort, bringing together the technical community, advertisers, publishers, and privacy experts, and the big data and privacy working group called for the initiative to continue its efforts. Disappointingly—and despite no downturn in consumer interest—there have been delays in moving this initiative forward. Stakeholders should recommit to developing new voluntary tools, including Do Not Track, to safeguard users' privacy.

Conclusion

Less than a year after the release of the big data and privacy working group's findings, the Obama Administration has made significant progress in furthering the majority of the recommendations made in the big data and privacy report. Policy development remains actively underway on complex recommendations, including extending more privacy protections to non-U.S. persons and scaling best practices in data management across government agencies. And in big data and discrimination, the civil rights and privacy communities will continue to play an active and critical role in driving the conversation, partnering with the federal government, and surfacing new issues for consideration in this new field.

Beyond the conclusions of the big data and privacy working group, the insights in the report have also had influence on Administration policy. In his State of the Union address, President Obama announced an ambitious plan to advance understanding of precision medicine, an emerging field that holds the promise of revolutionizing how we improve health and treat disease. Leveraging advances in genomics, clinical practice, big data technology, and other fields, the Precision Medicine Initiative will seek to create a one-million-strong national research cohort and to accelerate discovery of tailored treatments for cancers. Data security and patient privacy will be paramount to the Precision Medicine Initiative. The effort will incorporate the lessons learned by other federal agencies and the issues identified in the big data and privacy report and solicit input from a diverse range of privacy stakeholders from the earliest days in order to integrate rigorous privacy protections throughout the program.

The big data and privacy working group concluded that, despite the newness of the field, big data is already saving lives, making the economy and the government work better, and saving taxpayer dollars along the way. Big data will continue to contribute to and shape our society, and the Obama Administration will continue working to ensure that government and civil society strive to harness the power of these technologies while protecting privacy and preventing harmful outcomes.

SST Joint Research & Technology and Oversight Hearing
“Can Americans Trust the Privacy and Security of their Information on HealthCare.Gov?”
February 26, 2015
Rep. Elizabeth H. Esty Statement for the Record

Thank you to the Committee for holding this hearing on privacy and security concerns on HealthCare.Gov, and thank you to our witnesses for your time. Since so much of our personal business—from paying our credit cards to applying for mortgages to choosing health insurance—is now conducted online, it is all the more important that we maintain a strong cyber infrastructure to protect our security and personal privacy.

In Connecticut, we established our own health insurance marketplace, Access Health CT, for residents to shop for and secure health insurance. Over half a million Connecticut residents have already enrolled in health insurance plans through Access Health CT, and in 2014 our state’s uninsured rate was cut in half. I am encouraged by the level of success we have achieved in Connecticut, and I look forward to working with my fellow Committee Members to ensure that Americans across the country have access to affordable healthcare without compromising their privacy and personal information.